UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

A OBTENÇÃO DE PROVAS ATRAVÉS DE BUSCA NO SMARTPHONE – DA RELATIVIZAÇÃO DO DIREITO AO SILÊNCIO

MESTRADO CIENTÍFICO EM DIREITO

ESPECIALIDADE EM CIÊNCIAS JURÍDICO-CRIMINAIS

PERFIL DE DIREITO PENAL E CIÊNCIAS CRIMINAIS

HUMBERTO ALEXANDRE CAMPOS RAMOS

Lisboa

2018

UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

A OBTENÇÃO DE PROVAS ATRAVÉS DE BUSCA NO SMARTPHONE – DA RELATIVIZAÇÃO DO DIREITO AO SILÊNCIO

Dissertação de Mestrado apresentada ao curso de Mestrado em Ciências Jurídico-Criminais da Faculdade de Direito da Universidade de Lisboa, para a obtenção do título de Mestre, sob a orientação do Senhor Professor Doutor Augusto Silva Dias.

HUMBERTO ALEXANDRE CAMPOS RAMOS

Lisboa

2018

Coração civil

Quero a utopia, quero tudo e mais
Quero a felicidade dos olhos de um pai
Quero a alegria muita gente feliz
Quero que a justiça reine em meu país
Quero a liberdade, quero o vinho e o pão
Quero ser amizade, quero amor, prazer
Quero nossa cidade sempre ensolarada
Os meninos e o povo no poder, eu quero ver
São José da Costa Rica, coração civil
Me inspire no meu sonho de amor Brasil
Se o poeta é o que sonha o que vai ser real
Bom sonhar coisas boas que o homem faz
E esperar pelos frutos no quintal
Sem polícia, nem a milícia, nem feitiço, cadê poder?
Viva a preguiça, viva a malícia que só a gente é que sabe ter
Assim dizendo a minha utopia eu vou levando a vida
Eu vou viver bem melhor
Doido pra ver o meu sonho teimoso, um dia se realizar
Milton Nascimento/Fernando Brant

Agradecimentos

Ao Pai;
Aos meus pais, José e Angelina, que me incutiram o amor aos livros;
Aos meus filhos, Leonardo e Mariana, meu orgulho, meu legado;
Aos meus assessores, Diego e Ana Paula;
Ao meu genro Douglas, incentivador de todas as horas;
Ao Ministério Público do Estado do Espírito Santo.
Dedico a presente a minha mulher Wânia Maria, meu esteio, meu amor, sem a qual a vida não teria sentido.

RESUMO:

A presente dissertação tem por objetivo abordar a partir de uma decisão emitida pelo Juiz Steven Frucci no estado de Virginia/USA, no sentido de que as pessoas não têm de desbloquear seu smartphone protegido por senha para a polícia do estado, porém, no caso dos smartphones protegidos por digitais e senhas a problemática alusiva a autoincriminação referente a colheita de provas obtidas em aparelhos dessa natureza de propriedade do arguido à sua revelia e sem a devida autorização judicial, bem como as consequências jurídicas que podem advir de tal fato em relação a garantia de não autoincriminação e ao direito ao silêncio, sobretudo no que diz respeito a eventual violação ao princípio *nemo tenetur* se detegere, fazendo uma breve análise do caso concreto. Este assunto já é motivo de grande preocupação por parte da doutrina criminal em face do avanço da tecnologia. Tecemos comentários acerca do protagonismo e da importância que a criptografia exerce no tema. A dificuldade de se "quebrar" as senhas e as formas de criptografia utilizadas. Procuramos, também, contextualizar o assunto jurisprudencialmente. Ressaltamos os princípios que informam o tema, a quebra de sigilo de dados e sua influência na intimidade e na vida privada das pessoas. O direito ao silêncio como garantia a não autoincriminação e a fragilidade dessa garantia no direito atual. A produção de provas do arguido contra si mesmo, e as provas ilícitas por derivação, abordando a teoria dos frutos da árvore envenenada e seu nexo de causalidade com o *nemo tenetur.* Tecemos, ainda que, de passagem, breves comentários sobre a teoria da conclusão antecipada (foregone conclusion). Abordamos, ainda, o direito ao silêncio, de *per si* e sua relativização. A relação entre a globalização do terrorismo, as providências que os organismos internacionais têm adotado para combate-lo e suas consequências nefastas paro o direito de permanecer em silêncio.

PALAVRAS-CHAVE:

SMARTPHONE. AUTOINCRIMINAÇÃO. PROVAS PRODUZIDAS PELO PROPRIO ARGUÍDO. AUTOINCRIMINAÇÃO E RELATIVIZAÇÃO DO DIREITO AO SILÊNCIO.

ABSTRACT

The present dissertation aims to address a decision issued by Judge Steven Frucci in the state of Virginia / USA, in the sense that people do not have to unlock their password protected smartphone for state police, but in the case of smartphones protected by digital and passwords the problematic allusive to self-incrimination regarding the collection of evidence obtained in devices of this nature owned by the defendant in his her absence and without the due judicial authorization, as well as the legal consequences that may result from this fact in relation to the guarantee of non-self-incrimination and the right to silence, especially as regards any breach of the principle nemo tenetur se detegere, giving a brief analysis of the case. This subject is already cause for great concern on the part of criminal doctrine in the face of the advancement of technology. We have comments about the leading role and importance of encryption in the subject. The difficulty of "breaking" the passwords and the forms of encryption used. We also seek to contextualize the matter jurisprudentially. We emphasize the principles that inform the subject, the breach of secrecy of data and its influence in the intimacy and the private life of the people. The right to silence as a guarantee of non-self-incrimination and the fragility of this guarantee in current law. The production of evidence of the defendant against himself, and the illicit evidence by derivation, addressing the theory of the fruits of the poisoned tree and its nexus of causality with nemo tenetur. We write, however, in passing, brief comments on the theory of foregone conclusion. We also address the right to silence, per se and its relativization. The relationship between the globalization of terrorism, the measures that international bodies have taken to combat it, and its nefarious consequences stand for the right to remain silent.

KEYWORDS:

SMARPHONE. SELF INCRIMINATION. EVIDENCES PRODUCED BY HIMSELF AND THE RIGHT TO REMAIN SILENCE

ÍNDICE

Introdução[1]

A partir da criação de novas formas de tecnologia, sobretudo referente a área de comunicação, com a introdução da internet e aparelhos de telefonia celular, surgiram novas demandas, exigindo do profissional em Direito respostas claras e eficientes em matérias desse jaez. Nesse prisma, ante a grande velocidade em inovações técnicas, o contexto mundial exige que demandas sejam resolvidas de forma imediata, sob pena de perecer questões caríssimas em relação ao contexto social em que estamos inseridos.

Diante de tais assertivas, torna-se claro a necessidade imperiosa de que, se há violação a determinado bem jurídico, deve o Estado (Estado interno ou Estado nação) atuar com o propósito de lançar mecanismos a fim de proteger e resguardar eventuais bens jurídicos violados. Do mesmo modo em que os aparelhos de telefonia e a internet servem para aproximar pessoas e ajudar na proliferação de conhecimento/notícias e outros, podem auxiliar os órgãos de acusação e de julgamento no que concerne a realização de um julgamento justo, utilizando informações obtidas em aparelhos de telefonia celular como meio de provas.

Nesse sentido, a tecnologia vem, a cada dia alterando profundamente o mundo e, via de consequência nossa relação com o mesmo. Não poderia ser diferente no ambiente jurídico, sobretudo no âmbito do Direito Penal, onde os meios de obtenção de prova têm possibilitado a apuração mais acurada da autoria delituosa.

Hoje temos câmeras espalhadas por todos os cantos do planeta.

A garantia de não autoincriminação e o direito de permanecer em silêncio estão agonizando!

---

[1] Foram também utilizados como fonte o Relatório elaborado pelo autor na disciplina Direito Processual Penal sob a Regência do Professor Dr. Paulo Sousa Mendes, com o mesmo título do presente no ano de 2015 (com a autorização do Professor Orientador) e a dissertação de mestrado intitulada: A necessidade de desencriptação de smartphones para obtenção de provas no processo penal: restrições ao princípio da não autoincriminação na era digital de autoria da Dra. Vanessa Fernandes, orientada pelo Professor Dr. Paulo Sousa Mendes, no ano de 2017.

Com o advento dos séculos XX e XXI, novas questões de extrema relevância vão se impondo a análise dos legisladores, juristas e profissionais de várias outras áreas afins e não afins.

Nesta dissertação, analisaremos a questão da possibilidade de uso, como prova, das informações contidas nos *smartphones* protegidos através da biometria (impressões digitais) e senhas numéricas e que possam ter conteúdo capaz de incriminar seu possuidor, bem como a relativização do direito de permanecer em silêncio em face da nova ordem mundial.

Conforme declarou a Juíza da Suprema Corte Americana Elena Kagan[2], "A maioria das pessoas agora transportam suas vidas em *smartphones*. Isto é possível graças a enorme capacidade de armazenamento de dados que podem conter tais instrumentos, bem como pela facilidade em trazê-los consigo em face de sua portabilidade.

Um smartphone, hoje, possui mais tecnologia que o foguete Apolo XI, apenas para dimensionar a quantidade de informações que pode conter um pequeno aparelho.

Em 2012, o Presidente da Suprema Corte Americana, John D. Roberts Jr, declarou em uma palestra na Universidade de Rice que "a Suprema Corte deve identificar o princípio fundamental adjacente à proteção constitucional, o que é, e aplicá-lo a novas questões e novas tecnologias". Segundo ele, este "vai ser o verdadeiro desafio para os próximos 50 anos".

A questão, *sub examen* traz tamanhas indagações que foi objeto de matéria de cunho jornalístico no site CONJUR, em 03/12/2013, de autoria de João Ozório de Melo[3].

---

[2] http://www.conjur.com.br/2013dez03/direitosindividuais versus novas tecnologias são desafio justice eua

[3] Melo, João Ozório de - Legislativo que não legisla não é privilégio dos Estados Unidos. Legislativo que não legisla não é privilégio dos Estados Unidos. Mas a pressão no país para adequar as leis — e até mesmo a Constituição — à era digital está muito alta. A cada avanço da tecnologia, mais o vácuo jurídico se amplia, criando territórios sem lei, sem disposições constitucionais e sem casos anteriores para orientar a Justiça.

Por isso, a população americana está depositando toda a sua esperança no Judiciário. Na próxima semana, a Suprema Corte dos EUA começa a decidir se aceita ou não examinar algumas questões jurídicas relacionadas a novas tecnologias e, com isso, "salvar os tribunais, que estão muito confusos, tomando decisões opostas ou se recusando a tomar qualquer decisão", segundo o site Político.

Há dúvidas. Os ministros são avessos à tecnologia, como disse a ministra Elena Kagan recentemente. Em setembro, o ministro Antonin Scalia disse, em uma palestra, que a Suprema Corte terá, em algum momento, de decidir sobre o programa de vigilância do governo americano, por exemplo. Para ele, isso é ruim, porque o Judiciário é o braço do governo que menos entende de alta tecnologia.

A maior preocupação da população americana, bem como da comunidade jurídica (incluindo os juízes), é com o confronto entre direitos constitucionais — direito à privacidade, direito de não se autoincriminar, proteção contra buscas e apreensões sem mandado judicial — e o trabalho dos órgãos de segurança, da Polícia à Agência Nacional de Segurança (NSA).

Um dos casos chegou à Suprema Corte graças a uma certa "interferência" da chefe de um tribunal federal de recursos, a juíza Sandra Lynch. Em um caso em que os demais ministros do tribunal decidiram rejeitar um processo que envolvia "a interseção entre a privacidade individual e a tecnologia em constantes avanços", ela escreveu: "Somente a Suprema Corte poderá finalmente resolver essas questões e eu espero que ela o faça".

O primeiro caso que a corte vai examinar levanta questões sobre a semelhança entre um telefone celular e um maço de cigarros. Há 40 anos, policiais revistaram um "suspeito" e encontraram uma certa quantidade de drogas escondidas em um maço de cigarro. Antes disso, a Suprema Corte havia decidido que a Polícia poderia fazer buscas em contêineres, sem mandado judicial. A questão era se um maço de cigarros equivalia a um contêiner. "Agora é se a busca em um celular equivale à busca em um maço de cigarro", disse ao jornal o advogado Hanni Fakhoury, da Electronic Frontier Foundation.

Em outras palavras, qual é a extensão da busca que é permitida à Polícia quando apreende um celular após uma prisão. Um tribunal de Massachusetts decidiu que a Polícia só pode verificar os registros telefônicos. Mas pode fazer uma busca em aplicativos? E se a pessoa tem um Dropbox? A Polícia pode acessar todos os arquivos? E os documentos que estão arquivados em nuvem? A Polícia pode olhar tudo? Não há lei que ajude a responder a essas perguntas.

Enquanto isso, os tribunais tomam decisões diferentes, às vezes opostas. De acordo com um levantamento da Electronic Frontier Foundation e da revista Forbes, tribunais de seis estados decidiram que a Polícia precisa de um mandado judicial para fazer busca em tecnologias de "suspeitos". No entanto, tribunais de outros 20 estados decidiram que a Polícia pode fazer essas buscas sem mandado. Se não há orientação jurídica, os juízes decidem como querem.

Em outro caso, a Polícia de Fronteiras fez uma busca em um laptop de um viajante e encontrou pornografia infantil. As autoridades policiais nas fronteiras podem examinar toda a bagagem dos viajantes sem mandado judicial. O advogado do suspeito questionou, na Justiça, se essa autorização para fiscalizar a bagagem se estende a dispositivos que os viajantes portam naturalmente.

O juiz que examinou o caso concluiu que os policiais estavam errados. "O presente caso ilustra esse aspecto único de dados eletrônicos. (...) É como se a busca em uma mala da pessoa pudesse revelar tudo o que ela está carregando nessa viagem e tudo que ela carregou em viagens passadas, porque é assim que um computador funciona: mesmo o que já foi apagado pode ser descoberto", escreveu a juíza Margaret McKeown. "Imagine se o governo tiver o direito de fazer buscas em dados arquivados em nuvem. Será muito mais problemático", disse.

Qual é sua senha, por favor?

Mesmo que a Polícia obtenha mandado de busca e apreensão de um disco rígido, ainda terá de lidar, hoje em dia, com criptografia e senhas. Os investigadores policiais terão de pedir ao suspeito: "O senhor pode nos fornecer sua senha, por favor? Pode desbloquear a conta e descriptografar os arquivos? Do contrário, não poderemos encontrar provas para incriminá-lo". A Polícia pode obrigar um "suspeito" a fazer qualquer dessas coisas?

Alguns tribunais têm decidido, em alguns casos, que as pessoas podem se recusar a fornecer sua senha, desbloquear contas ou descriptografar arquivos, porque fazer isso equivale a se autoincriminar — e é um direito constitucional do cidadão não se autoincriminar (Quinta Emenda da Constituição americana).

Em 2012, um tribunal federal decidiu que um suspeito pode "invocar a Quinta Emenda para não fornecer sua senha ou qualquer outra coisa que dê acesso à Polícia a seus arquivos porque, se fizer isso, será a

A busca em um *smartphone*, com certeza, encontrará um número enorme de informações, quer de natureza pública, quer privada, dentre essa infinidade de dados, eventualmente, um ou alguns dados poderão ter natureza autoincriminatória.

Os dispositivos móveis atuais funcionam de forma similar ao computador: possuem processador, memória RAM (utilizada para armazenar dados que estão em uso pelo

---

mesma coisa que testemunhar que o material encontrado em seu disco rígido pertence a ele". Isso é autoincriminação.
Em um caso na Suprema Corte de Massachusetts, um advogado foi acusado de fraude no sistema de financiamento habitacional e a Polícia foi à sua casa e confiscou computadores e outros dispositivos eletrônicos. Mas não pôde ver os arquivos porque estavam criptografados. A Polícia argumenta que há provas do crime nos computadores, mas a defesa alega que os policiais não têm provas do que o computador contém. A única prova que têm é que o advogado comprou aqueles computadores.
"Há dois meses, a Apple lançou um iPhone que o proprietário pode bloquear e desbloquear com sua impressão digital. Em pouco tempo, haverá tecnologia que permite ao usuário fazer isso com os olhos. Como os tribunais vão lidar com isso, se não conseguem decidir questões bem mais simples, porque não há leis que os oriente?", pergunta Fakhoury.
Localização do celular
No ano passado, a Suprema Corte decidiu que a Polícia — ou qualquer órgão de segurança — não pode fixar um GPS no carro de uma pessoa investigada sem mandado judicial, para seguir seus movimentos, observar os lugares que frequenta etc. Isso seria invasão de propriedade particular. Mas, aparentemente, o mesmo raciocínio não se aplica quando a Polícia segue os deslocamentos de um suspeito com a ajuda de sua provedora de serviços, que tem capacidade de rastrear o telefone celular ou smartphone da pessoa.
Os tribunais estão divididos sobre esse assunto. Mais recentemente, um tribunal de recursos do Texas decidiu que a Polícia pode obter dados de rastreamento de celulares das provedoras de serviços, sem mandado judicial. A Suprema Corte de Nova Jersey decidiu exatamente o contrário: é preciso obter um mandado, de acordo com a Constituição do estado.
Doutrina dos terceiros
Em 1970, a Suprema Corte decidiu que, quando uma pessoa confia informações a terceiros, como um banco ou uma companhia telefônica, ela abre mão de seus direitos de manter essas informações privadas, fora do alcance do governo. A decisão ficou conhecida como a "doutrina dos terceiros". Para muitos juristas, o problema é que essa decisão foi tomada muito antes da existência da Internet e dos smartphones. "Naquela época, os dados eram anotados à caneta, em papéis. É muito diferente do volume de dados que os usuários enviam eletronicamente, hoje, às provedoras de serviço".
"O que resta aos juízes fazer, por falta de legislação atualizadas, é ligar casos novos a casos velhos — e a cada dia mais velhos, porque a tecnologia evolui rapidamente", diz o advogado Alan Butler, do Centro para a Privacidade das Informações Eletrônicas.
Alguém pode processar a NSA? Não. A NSA pode espionar quem quiser, sem problemas judiciais. "A Quarta Emenda da Constituição, que garante ao cidadão proteção contra buscas e apreensões não razoáveis, sem mandado judicial, não faz qualquer menção ao programa de metadados operado pela NSA", diz o professor da Faculdade de Direito de Vanderbilt Christopher Slobogin, porque todas as comunicações por telefone ou e-mail são confiadas a terceiros — a empresa provedora. E, portanto, caem na "doutrina dos terceiros".

Além disso, no ano passado, a Suprema Corte decidiu, depois das revelações do ex-agente da CIA Edward Snowden, que uma pessoa tem de provar que está sendo vigiado pela NSA, para poder processá-la. "É uma pegadinha", diz Slobogin. "Para processar a NSA, você têm de pedir à NSA que lhe confirme que está sendo vigiado".

processador) e área de armazenamento de dados (utilizada para armazenar dados de forma duradoura). Além de a parte física ser concebida de forma similar, os sistemas operacionais destes aparelhos possuem os mesmos conceitos dos utilizados em computadores, alguns, inclusive, utilizam o mesmo núcleo, como é o caso do Android que utiliza o Linux. Desta forma, diversas perícias que anteriormente eram feitas apenas em computadores, hoje em dia são feitas em *smartphones* e *tablets* com a mesma eficiência.

O sistema operacional possui diversos procedimentos que são executados sem o conhecimento do usuário, um profissional que detenha essa expertise poderá se valer de tal conhecimento para recuperar muitas informações como arquivo, áudios, vídeos, fotos e até mesmo um histórico de atividades realizadas pelo indivíduo.

Por exemplo, no sistema Android, fotos enviadas pelo aplicativo WhatsApp ficam armazenadas em uma pasta separada dentro da área de armazenamento de dados. Caso o indivíduo envie uma imagem e logo em seguida a apague da sua “Galeria de Fotos”, esta imagem permanecerá salva em outro local sem que o usuário tenha feito alguma ação para tal, possibilitando assim a recuperação.

Além disso, hoje em dia é possível gravar um histórico de localização do aparelho, ou seja, pode-se ver o deslocamento que o aparelho teve pela cidade em um determinado dia e horário, deduzindo que o aparelho sempre acompanha o dono, obtém-se o deslocamento do proprietário. O objetivo é que essas informações sejam utilizadas em benefício próprio, mas em poder de criminosos poderiam ser o ponto de partida para uma extorsão.

Como funcionam similarmente a um computador convencional, os dispositivos móveis possuem muitas proteções semelhantes: antivírus, antimalwares, firewalls, aplicativos de proteção de dados e criptografia são alguns exemplos.[4]

---

[4] Carneiro, Leandro Dias, Infrações penais e a informática: a tecnologia como meio para o cometimento de crimes, Revista Âmbito Jurídico - No 168 - Ano XX - ABRIL/2018 - ISSN - 1518-0360

Face à incapacidade e dificuldade do legislador em enfrentar e acompanhar os problemas decorrentes da enorme rapidez com que surgem novas tecnologias, bem como a proteção dessas informações contidas nos *smartphones* através de mecanismos criados pelos programadores visando a proteção da privacidade e intimidade de seus proprietários, pode-se afirmar que, em um primeiro momento, a resolução de pendências oriundas da tecnologia, mais o vácuo jurídico se amplia, criando territórios sem lei, sem disposições constitucionais e sem casos anteriores para orientar a Justiça.

Há dúvidas. Os ministros são avessos à tecnologia, como disse a ministra Elena Kagan recentemente. Em setembro, o ministro Antony Scalia disse, em uma palestra, que a Suprema Corte terá, em algum momento, de decidir sobre o programa de vigilância do governo americano, por exemplo. Para ele, isso é ruim, porque o Judiciário é o braço do governo que menos entende de alta tecnologia.

A maior preocupação da população americana, bem como da comunidade jurídica (incluindo os juízes), é com o confronto entre direitos constitucionais — direito à privacidade, direito de não se autoincriminar, proteção contra buscas e apreensões sem mandado judicial — e o trabalho dos órgãos de segurança, da Polícia à Agência Nacional de Segurança (NSA).

Enquanto isso, os tribunais tomam decisões diferentes, às vezes opostas. De acordo com um levantamento da Electronic Frontier Foundation e da revista Forbes, tribunais de seis estados decidiram que a Polícia precisa de um mandado judicial para fazer busca em tecnologias de "suspeitos". No entanto, tribunais de outros 20 estados decidiram que a Polícia pode fazer essas buscas sem mandado. Se não há orientação jurídica, os juízes decidem como querem.
Qual é sua senha, por favor?

Mesmo que a Polícia obtenha mandado de busca e apreensão de um disco rígido, ainda terá de lidar, hoje em dia, com criptografia e senhas. Os investigadores policiais terão de pedir ao suspeito: "O senhor pode nos fornecer sua senha, por favor? Pode desbloquear a conta e descriptografar os arquivos?

Do contrário, não poderemos encontrar provas para incrimina-lo". A Polícia pode obrigar um "suspeito" a fazer qualquer dessas coisas? Alguns tribunais têm decidido, em alguns casos, que as pessoas podem se recusar a fornecer sua senha, desbloquear contas ou descriptografar arquivos, porque fazer isso equivale a se auto incriminar e é um direito constitucional do cidadão não se auto incriminar (Quinta Emenda da Constituição americana).

Em 2012, um tribunal federal decidiu que um suspeito pode "invocar a Quinta Emenda para não fornecer sua senha ou qualquer outra coisa que dê acesso à Polícia a seus arquivos porque, se fizer isso, será a mesma coisa que testemunhar que o material encontrado em seu disco rígido pertence a ele". Isso é autoincriminação.

Situações que tenham relevância penal, sejam objeto de análise dos Tribunais, a quem caberá, caso a caso, apresentar soluções para as demandas dessa natureza.

Em decorrência de tais fatos, alguns conceitos devem ser analisados para possibilitar maior entendimento sobre o tema.

As Constituições Portuguesa (artigo 26), Brasileira (artigo 5º, X e LVII) Americana (4ª e 5ª emendas) a Declaração Universal de Direitos do Homem (artigo 12), bem como a grande maioria dos países democráticos abordam estes assuntos, quer como princípios, quer como garantias ou direitos fundamentais. [5]

---

[5] Constituição Portuguesa Artigo.26
Outros direitos pessoais
1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação.

O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas.

1 - Da Análise do Caso Concreto

Em fevereiro de 2014, a imprensa americana divulgou uma decisão emitida pelo Juiz Steven Frucci no estado de Virginia no sentido de que as pessoas não têm de desbloquear seu smartphone protegido por senha para a polícia do estado, porém, no caso dos smartphones protegidos por digitais e senhas alfanuméricas a situação é diferente.

Tal fato ocorreu no caso em que um paramédico tentou estrangular sua namorada (Commomwealth of Virginia v. David Charles Baust).

---

2. A lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.
3. A lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica.
4. A privação da cidadania e as restrições à capacidade civil só podem efectuar-se nos casos e termos previstos na lei, não podendo ter como fundamento motivos políticos.

Constituição Brasileira
Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
LVII - ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória;

Constituição Americana
EMENDA IV

O Ministério Público, na tentativa de incriminar o suposto autor do delito requisitou ao Juiz acesso ao smartphone do mesmo que, supostamente, continha as imagens do ato criminoso, posto que, no quarto onde ocorreu o crime, havia um sistema de vigilância que transmitiria as imagens colhidas para o referido aparelho e que poderia ter registrado o incidente. Tal smartphone foi apreendido através de mandado judicial dias após o fato.

Certo é que o Ministério Público desconhecia se o smartphone continha as imagens e tentava, com seu requerimento, tal esclarecimento.

Certo é, também, que o referido aparelho era bloqueado biometricamente (através da digital) e possuía uma senha numérica, e como o mesmo fora desligado, para se ter acesso às informações ali contidas seria necessário uso da impressão digital do suposto autor e, posteriormente de uma senha numérica para acessar os dados ali contidos e que ocorridas mais de dez tentativas equivocadas na inserção da password, tais eventuais dados seriam deletados.

A decisão judicial (Juiz Steven C. Frucci) foi no sentido de que obrigar o suspeito a fornecer sua senha numérica para quem quer que fosse, contra sua vontade, seria uma violação a 5ª emenda, porque forçaria o suspeito a se autoincriminar caso as imagens estivessem presentes, garantindo-lhe, dessa forma, o direito ao silêncio (de não testemunhar contra si próprio).

No entanto, complementando a decisão, determinou ao suspeito que fornecesse suas digitais para desbloquear o telefone, porque tal situação é similar ao fornecimento, de DNA, escrita para exame grafotécnico ou a chave de um cofre (sem o segredo) e, sempre, através de mandado.[6]

---

[6] Bressan, Kelvin J. É necessária autorização judicial para exame dos dados armazenados em um smartphone?: emporiododireito.com.br/leitura/e-necessaria-autorizacao-judicial-para-exame-dos-dados-armazenados-em-um-smartphone-uma-breve-analise-do-rhc-n-51-531-ro-do-superior-tribunal-de-justica Uma breve análise do RHC n. 51.531/RO, do Superior Tribunal de Justiça. No dia 19 de abril de 2016, a Sexta Turma do Superior Tribunal de Justiça deu provimento ao Recurso Ordinário em Habeas Corpus n. 51.531/RO para declarar como ilícitas as provas obtidas a partir do celular do paciente sem prévia ordem

judicial. A decisão, disponibilizada no site do Tribunal no dia 9 de maio de 2016, recebeu a seguinte ementa:

PENAL. PROCESSUAL PENAL. RECURSO ORDINÁRIO EM HABEAS CORPUS. TRÁFICO DE DROGAS.

NULIDADE DA PROVA. AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL PARA A PERÍCIA NO CELULAR. CONSTRANGIMENTO ILEGAL EVIDENCIADO. 1. Ilícita é a devassa de dados, bem como das conversas de whatsapp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial.2. Recurso ordinário em habeas corpus provido, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos.

II - Sobre o caso

O Recorrente foi preso em flagrante após a Polícia Militar encontrá-lo na posse de 300 (trezentos) comprimidos de ecstasy, remetidos a ele, supostamente, pela via postal[1]. Apreendido seu aparelho celular, as informações contidas no dispositivo (fotos e conversas pelo aplicativo whatsapp) foram acessadas pela Autoridade Policial sem prévia autorização judicial.[2]

Instado, o Tribunal de Justiça do Estado de Rondônia assentou ser "[...] válida a transcrição de mensagens de texto gravadas no aparelho celular apreendido com o paciente por ocasião de sua prisão em flagrante pois estes dados não gozam da mesma proteção constitucional de que trata o art. 5º, XII" (Habeas Corpus n. 000708393.2014.822.0000, 2ª Câmara Criminal, Relator Des. Valdeci Castellar Citon. Data do julgamento: 6/8/2014).

III - O refinamento do precedente gravado no HC n. 91.867/PA, do Supremo Tribunal Federal, e o panorama internacional sobre a questão.

Julgando fatos ocorridos no ano de 2004, o Supremo Tribunal Federal entendeu inexistir coação ilegal no fato de a Autoridade Policial, desprovida de qualquer ordem judicial, ter procedido à análise do registro telefônico de dois celulares após a prisão em flagrante de um suspeito.[3]

Cientes de tal precedente, os Ministros expressaram em seus respectivos votos que a atual quadra do desenvolvimento tecnológico permite que um smartphone armazene uma imensa quantidade de informações sobre a vida privada do seu proprietário, não se resumindo, como nos idos de 2004, ao simples registro de ligações e agenda de contatos. Nas palavras da Ministra Maria Thereza de Assis Moura (p. 2 do seu voto):

[...] existe uma infinidade de dados privados que, uma vez acessados, possibilitam uma verdadeira devassa na vida pessoal do titular do aparelho.

É inegável, portanto, que os dados constantes nestes aparelhos estão resguardados pela cláusula geral de resguardo da intimidade, estatuída no artigo 5º, X, da Constituição. A proteção dos dados armazenados em aparelhos celulares, portanto, é ínsita ao direito fundamental à privacidade.

O Relator, Ministro Nefi Cordeiro, equiparou a proteção aos dados armazenados no aparelho celular à que gozam o sigilo bancário, telefônico e de correio eletrônico, ou seja: somente podem ser acessados por prévia e fundamentada decisão judicial (p. 5-6 do seu voto).

O Ministro Rogério Schietti Cruz bem lembrou que existem dois tipos de dados protegidos quando se acessa o aparelho celular: aqueles já gravados no aparelho e os que eventualmente sejam interceptados durante o manuseio (p. 7-8 do voto).

Os citados Ministros levaram a discussão para o cenário internacional ao apresentarem o entendimento da

Suprema Corte dos Estados Unidos da América, representado pelo caso Riley vs. California (573 U.S. 2014), no sentido de que é exigida ordem judicial prévia para que a Autoridade Policial possa acessar os dados de um aparelho celular apreendido (p. 4 e p. 9-10 do respectivo voto, na ordem de citação).

A Ministra Maria Thereza foi além e mencionou recente decisão proferida pela Suprema Corte do Canadá (R. v. Fearon, 2014, SCC 77, 2014, S.C.R. 621) legitimando o acesso da polícia aos dados armazenados em um celular independentemente de autorização judicial, desde que: a) a prisão tenha sido lícita; b) o acesso aos dados ocorra incidental e imediatamente após a prisão, demonstrada a necessidade da medida em relação à persecução penal (v.g. proteger a autoridade policial, o suspeito ou o público; preservar elementos de prova; e/ou descobrir novas provas caso a investigação possa resultar impedida ou prejudicada significativamente); c) via de regra, apenas emails, textos e fotos e chamadas telefônicas sejam verificadas; d) a Autoridade Policial reporte como e quais dados foram acessados, aplicativos verificados, duração e extensão do exame.

Ainda, trouxe à baila o entendimento do Tribunal Constitucional Espanhol (Sentencia 115/2013) – semelhante ao do Supremo Tribunal Federal no HC n. 91.867/PA – que, ao valer-se do princípio da proporcionalidade, considerou como uma "ingerência leve" a consulta da agenda telefônica de um celular abandonado por suspeitos em fuga. O Tribunal, porém, deixou claro que uma análise mais aprofundada dos dados encontrados no aparelho implicaria em maior rigor na ponderação.

Finalmente, a Ministra fundamentou seu voto em um juízo de proporcionalidade entre a garantia geral de segurança pública (art. 144 da Constituição Federal)[4] e o direito à privacidade (art. 5.º, X, da Constituição Federal), consignando não verificar urgência ou excepcionalidade que permitisse à Autoridade Policial ter acesso imediato aos dados constantes no smartphone do Recorrente, de modo que (p. 7 do voto):

Diante da situação concreta posta no presente recurso, para a validade da obtenção dos dados caberia às autoridades policiais realizar imediatamente a apreensão do aparelho e postular ao Poder Judiciário, subsequentemente, a quebra de sigilo dos dados armazenados no aparelho celular. Não tendo assim procedido, a prova foi obtida de modo inválido, devendo ser desentranhada dos autos, nos termos do artigo 157 do Código de Processo Penal.

IV - Conclusão

Numa perspectiva geral, andou bem o Superior Tribunal de Justiça em sua decisão. O reconhecimento de que os dados armazenados em um smartphone devem integrar a proteção à intimidade de toda e qualquer pessoa é, sem dúvida, um necessário e acertado avanço.

Todavia, não se pode ignorar a "carta coringa" presente no voto da Ministra Maria Thereza de Assis Moura por conta da utilização do princípio da proporcionalidade (R. Alexy) como critério de decisão. Nas palavras da Ministra (p. 7 do seu voto):

Não descarto, de forma absoluta, que, a depender do caso concreto, caso a demora na obtenção de um mandado judicial pudesse trazer prejuízos concretos à investigação ou especialmente à vítima do delito, mostre-se possível admitir a validade da prova colhida através do acesso imediato aos dados do aparelho celular. Imagine-se, por exemplo, um caso de extorsão mediante sequestro, em que a polícia encontre aparelhos celulares em um cativeiro recém-abandonado: o acesso incontinenti aos dados ali mantidos pode ser decisivo para a libertação do sequestrado.

Não ignoramos a gravidade da situação posta pela Ministra, porém, adiantar um juízo de proporcionalidade parece, no mínimo, temerário, mormente em tempos de crescentes desejos punitivistas, abrindo margem para atuações abusivas disfarçadas de "proporcionais".

Ademais, como bem leciona Lopes Jr[5], o conceito de proporcionalidade é francamente manipulado e "[...] serve a qualquer senhor". Com o fito de objurgar direitos fundamentais do réu, esse pensamento opera em um reducionismo binário de interesse público x interesse privado, vendo a sociedade como um ser gigantesco e superior da qual todos os homens dependem e devem obediência, deixando de lado a atual complexidade das relações sociais, constituindo-se, pois, em uma visão autoritarista e que não pode mais ser aceita.

Vale colacionar outra importante observação do professor Lopes Jr[6]:

[...] em matéria penal, todos os interesses em jogo – principalmente os do réu – superam muito a esfera do "privado", situando-se na dimensão de direitos fundamentais (portanto, "público", se preferirem). Na verdade, são verdadeiros direitos de todos e de cada um de nós, em relação ao (ab)uso de poder estatal.

Para finalizar, caro leitor, gostaríamos de compartilhar um exemplo da "sutileza" com que a violação ora combatida pode ocorrer[7]: Direito à privacidade sumariamente violado.

Notas e Referências:

[1] O paciente foi denunciado pela prática dos crimes previstos nos arts. 33 e 35 da Lei 11.343/06 e art. 329 doCP.

[2] Pela dinâmica do caso, muito embora não mencionado nos votos, é possível supor que as informações obtidasseriam utilizadas para provar a ocorrência do crime previsto no art. 35 da Lei n. 11.343/06.

[3] [...] 2. Ilicitude da prova produzida durante o inquérito policial - violação de registros telefônicos de corréu, executor do crime, sem autorização judicial. 2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode

2 - Breves comentários a respeito da criptografia[7]

---

interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito (dessa análise logrou encontrar ligações entre o executor do homicídio e o ora paciente). Verificação que permitiu a orientação inicial da linha investigatória a ser adotada, bem como possibilitou concluir que os aparelhos seriam relevantes para a investigação. [...]. (Habeas Corpus n. 91867, Relator Min. GILMAR MENDES, Segunda Turma. Data do julgamento: 24/4/2012. Sem grifos no original).

[4] Foram citados, ainda, dispositivos das Leis n. 9.472/97 e 12.965/14 (p. 6 do voto).

[5] LOPES JR, Aury. Direito processual penal. 10. ed. – São Paulo: Saraiva, 2013, p. 596-597.

[6] LOPES JR, Aury. Fundamentos do Processo Penal: introdução crítica. São Paulo: Saraiva, 2015, p. 34.

[7] Infelizmente, a violação à privacidade foi apenas um dos incontáveis “desvios” (nos faltam palavras paradescrever o que se passou na abordagem policial) registrados.

[7] OLIVEIRA, Ronielton Rezende. Criptografia tradicional simétrica de chave privada e criptografia assimétrica de chave pública: análise das vantagens e desvantagens. Niterói : Trabalho da pós-graduação Criptografia e Segurança em Redes da UFF, 2006. 20p. [1] Publicado na Revista online com distribuição gratuita Segurança Digital em duas partes: 5ª Edição – páginas 11 à 15 (31 de março de 2012) e 6ª Edição Criptografia simétrica e assimétrica: os principais algoritmos de cifragem[1] Ronielton Rezende Oliveira ronielton@ronielton.eti.br Resumo A palavra criptografia provém dos radicais gregos kriptos (oculto) e grapho (escrita) e é o nome dado à ciência ou arte de codificar mensagens usando uma fórmula, que também será utilizada depois para decodificar a mesma mensagem. Na criptografia moderna, esta fórmula é chamada de algoritmo. Usada há milênios pela humanidade, a criptografia se tornou essencial para garantir a privacidade das comunicações no mundo atual, principalmente em redes de computadores públicas como a internet, por onde circulam dados pessoais, comerciais, bancários e outros. Conhecer, difundir e utilizar algoritmos criptográficos é essencial ao profissional de Tecnologia da Informação que no mundo moderno, entre suas atribuições deve proteger e garantir a privacidade das transações comerciais realizadas através de meios eletrônicos, assim é fundamental o entendimento das técnicas, seus algoritmos, protocolos e finalmente a maneira como estes lidam com a informação a ser mantida segura. Palavras chave: Criptografia; Algoritmo; Segurança. 1. Introdução Quando falamos de informação e transportamos este conceito para o meio digital, particularmente na utilização das redes públicas de computação como a internet, e diversos são os serviços realizados é relevante ao ser humano à credibilidade nos sistemas computacionais, estes que inseridos nos fundamentos da segurança da informação, são definidos pela disponibilidade, integridade, controle de acesso, autenticidade, não-repudiação e finalmente a privacidade, os quais devem ser de livre compreensão e facilmente perceptíveis ao se efetuar transações computacionais: § Disponibilidade - garantir que uma informação estará disponível para acesso no momento desejado. § Integridade - garantir que o conteúdo da mensagem não foi alterado. § Controle de acesso - garantir que o conteúdo da mensagem somente será acessado por pessoas autorizadas. § Autenticidade - garantir a identidade de quem está enviando a mensagem. § Não-repudiação - prevenir que alguém negue o envio e/ou recebimento de uma mensagem. § Privacidade - impedir que pessoas não autorizadas tenham acesso ao conteúdo da mensagem, garantindo que apenas a origem e o destino tenham conhecimento. O exemplo clássico é uma compra pela internet, todos os requisitos são encontrados neste processo de troca de informações: A informação que permite a transação - valor e descrição do produto - precisa estar disponível no dia e na hora que o cliente desejar efetuá-la (disponibilidade), o valor da transação não pode ser alterado (integridade), somente o cliente que está comprando e o comerciante devem ter acesso à transação (controle de acesso), o cliente que está comprando deve ser realmente quem diz ser (autenticidade), o cliente tem como provar o pagamento e o comerciante não têm como negar o recebimento (não-repúdio) e o conhecimento do conteúdo da transação fica restrito aos envolvidos (privacidade). Assim é fundamental que técnicas computacionais sejam empregadas para que os requisitos de proteção da

informação sejam atendidos. Neste cenário apresentam-se os dois tipos básicos de criptografia: a simétrica ou chave privada, e a assimétrica ou chave pública. 2. Criptografia simétrica ou chave privada O modelo mais antigo de criptografia, em que a chave, isto é, o elemento que dá acesso à mensagem oculta trocada entre duas partes, é igual (simétrica) para ambas as partes e deve permanecer em segredo (privada). Tipicamente, esta chave é representada por uma senha, usada tanto pelo remetente para codificar a mensagem numa ponta, como pelo destinatário para decodificá-la na outra. Essencialmente, quando a origem (ALFA) cifra uma mensagem, ele utiliza um algoritmo de ciframento para transformar o conteúdo em claro da mensagem em texto cifrado. Quando o destino (BRAVO) decifra uma mensagem, ele utiliza o algoritmo de deciframento correspondente para converter o texto cifrado de novo em uma mensagem clara. Se um intruso (CHARLIE) conhecer o algoritmo de ciframento, ele poderia decifrar uma mensagem cifrada tão facilmente quanto o destino (BRAVO). A solução no uso da criptografia de chave privada propõe que quando a origem (ALFA) cifra uma mensagem, ele utilize um algoritmo de ciframento e uma chave secreta para transformar uma mensagem clara em um texto cifrado. O destino (BRAVO), por sua vez, ao decifrar a mensagem, utiliza o algoritmo de deciframento correspondente e a mesma chave para transformar o texto cifrado em uma mensagem em claro. O intruso (CHARLIE), por não possuir a chave secreta, mesmo conhecendo o algoritmo, não conseguirá decifrar a mensagem. A segurança do sistema passa a residir não mais no algoritmo e sim na chave empregada. É ela (chave privada) que agora, no lugar do algoritmo, deverá ser mantida em segredo pela origem (ALFA) e destino (BRAVO). A principal vantagem é a simplicidade, esta técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos. Entenda que se as chaves utilizadas forem complexas a elaboração de um algoritmo de chave privada se torna bastante fácil, porém as possibilidades de interceptação são correlatas aos recursos empregados, entretanto sua utilização é considerável no processo de proteção da informação, pois quanto mais simples o algoritmo, melhor é a velocidade de processamento e facilidade de implementação. O principal problema residente na utilização deste sistema de criptografia é que quando a chave de ciframento é a mesma utilizada para deciframento, ou esta última pode facilmente ser obtida a partir do conhecimento da primeira, ambas precisam ser compartilhadas previamente entre origem e destino, antes de se estabelecer o canal criptográfico desejado, e durante o processo de compartilhamento a senha pode ser interceptada, por isso é fundamental utilizar um canal seguro durante o compartilhamento, este independente do destinado à comunicação sigilosa, uma vez que qualquer um que tenha acesso à senha poderá descobrir o conteúdo secreto da mensagem. Outras lacunas são interpostas a este sistema: § Como cada par necessita de uma chave para se comunicar de forma segura, para um uma rede de n usuários precisaríamos de algo da ordem de n2 chaves, quantidade esta que dificulta a gerência das chaves; § A chave deve ser trocada entre as partes e armazenada de forma segura, o que nem sempre é fácil de ser garantido; § A criptografia simétrica não garante os princípios de autenticidade e não-repudiação. Tabela 1 - Principais algoritmos de chave privada ou criptografia simétrica Algoritmo Bits Descrição AES 128 O Advanced Encryption Standard (AES) é uma cifra de bloco, anunciado pelo National Institute of Standards and Technology (NIST) em 2003, fruto de concurso para escolha de um novo algoritmo de chave simétrica para proteger informações do governo federal, sendo adotado como padrão pelo governo dos Estados Unidos, é um dos algoritmos mais populares, desde 2006, usado para criptografia de chave simétrica, sendo considerado como o padrão substituto do DES. O AES tem um tamanho de bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 bits, ele é rápido tanto em software quanto em hardware, é relativamente fácil de executar e requer pouca memória. DES 56 O Data Encryption Standard (DES) foi o algoritmo simétrico mais disseminado no mundo, até a padronização do AES. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quadrilhões de combinações, seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na internet. O NIST que lançou o desafio mencionado, recertificou o DES pela última vez em 1993, passando então a recomendar o 3DES. 3DES 112 ou 168 O 3DES é uma simples variação do DES, utilizando o em três ciframentos suscessivos, podendo empregar uma versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão. IDEA 128 O International Data Encryption Algorithm (IDEA) foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas na maioria dos microprocessadores, uma implementação por software do IDEA é mais rápida do que uma implementação por software do DES. O IDEA é utilizado principalmente no mercado

financeiro e no PGP, o programa para criptografia de e-mail pessoal mais disseminado no mundo. Blowfish 32 a 448 Algoritmo desenvolvido por Bruce Schneier, que oferece a escolha, entre maior segurança ou desempenho através de chaves de tamanho variável. O autor aperfeiçoou o no Twofish. Twofish 128 É uma das poucas cifras incluídas no OpenPGP. O Twofish é uma chave simétrica que emprega a cifra de bloco de 128 bits, utilizando chaves de tamanhos variáveis, podendo ser de 128, 192 ou 256 bits. Ele realiza 16 interações durante a criptografia, sendo um algoritmo bastante veloz. A cifra Twofish não foi patenteada estando acessível no domínio público, como resultado, o algoritmo Twofish é de uso livre para qualquer um utilizar sem restrição. RC2 8 a 1024 Projetado por Ron Rivest (o R da empresa RSA Data Security Inc.) e utilizado no protocolo S/MIME, voltado para criptografia de e-mail corporativo. Também possui chave de tamanho variável. Rivest também é o autor dos algoritmos RC4, RC5 e RC6. CAST 128 É um algoritmo de cifra de bloco, sendo criado em 1996 por Carlisle Adams e Stafford Tavares. O CAST-128 é um algoritmo de Feistel, com 12 a 16 iterações da etapa principal, tamanho de bloco de 64 bits e chave de tamanho variável (40 a 128 bits, com acréscimos de 8 bits). Os 16 rounds de iteração são usados quando a chave tem comprimento maior que 80 bits. 3. Criptografia assimétrica ou chave pública Modelo de criptografia criado na década de 1970 - pelo matemático Clifford Cocks que trabalhava no serviço secreto inglês, o GCHQ - na qual cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública. Neste caso, as chaves não são apenas senhas, mas arquivos digitais mais complexos (que eventualmente até estão associados a uma senha). A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular. É com a chave privada que o destinatário poderá decodificar uma mensagem que foi criptografada para ele com sua respectiva chave pública. Para entender o conceito, basta pensar num cadeado comum protegendo um determinado bem. A mensagem é este bem, e o cadeado, que pode ficar exposto, é a chave pública. Apenas quem tiver uma chave particular (privada) que consiga abrir o cadeado poderá acessar a mensagem. A principal vantagem deste método é a sua segurança, pois não é preciso (nem se deve) compartilhar a chave privada. Por outro lado, o tempo de processamento de mensagens com criptografia assimétrica é muitas vezes maior do que com criptografia simétrica, o que pode limitar seu uso em determinadas situações. Essencialmente, o destino (BRAVO) e todos os que desejam comunicar-se de modo seguro geram uma chave de cifrамento e sua correspondente chave de decifрamento. Ele mantém secreta a chave de decifрamento, esta é chamada de sua chave privada. Ele torna pública a chave de cifрamento, esta é chamada de sua chave pública. A chave pública realmente condiz com seu nome. Qualquer pessoa pode obter uma cópia dela. O destino (BRAVO) inclusive encoraja isto, enviando-a para seus amigos ou publicando-a na internet. Assim, O intruso (CHARLIE) não tem nenhuma dificuldade em obtê-la. Quando a origem (ALFA) deseja enviar uma mensagem ao destino (BRAVO), precisa primeiro encontrar a chave pública dele. Feito isto, ela cifra sua mensagem utilizando a chave pública do destino (BRAVO), despachando-a em seguida. Quando o destino (BRAVO) recebe a mensagem, ele a decifra facilmente com sua chave privada. O intruso (CHARLIE), que interceptou a mensagem em trânsito, não conhece a chave privada do destino (BRAVO), embora conheça sua chave pública. Mas este conhecimento não o ajuda a decifrar a mensagem. Mesmo a origem (ALFA), que foi quem cifrou a mensagem com a chave pública do destino (BRAVO), não pode decifrá-la agora. A grande vantagem deste sistema é permitir a qualquer um enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens. O óbice deste sistema é a complexidade empregada no desenvolvimento dos algoritmos que devem ser capazes de reconhecer a dupla de chaves existentes e poder relacionar as mesmas no momento oportuno, o que acarreta num grande poder de processamento computacional. Tabela 2 - Principais algoritmos de chave pública ou criptografia assimétrica Algoritmo Descrição RSA O RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. Atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número. Isto é conhecido como fatoração. Por exemplo,

os fatores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia se na dificuldade de fatoração de números grandes. Deste modo, a fatoração representa um limite superior do tempo necessário para quebrar o algoritmo. Uma chave RSA de 512 bits foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 países. Levou cerca de 7 meses e foram utilizadas 300 estações de trabalho para a quebra. No Brasil, o RSA é utilizado pela ICP-Brasil, no seu sistema de emissão de certificados digitais, e a partir do dia 1º de janeiro de 2012, as chaves utilizadas pelas autoridades certificadoras do país, passam a serem emitidas com o comprimento de 4.096bits, em vez dos 2.048bits atuais. ElGamal O ElGamal é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração. Diffie-Hellman Também baseado no problema do logaritmo discreto, e o criptosistema de chave pública mais antigo ainda em uso. O conceito de chave pública, aliás foi introduzido pelos autores deste criptosistema em 1976. Contudo, ele não permite nem ciframento nem assinatura digital. O sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público. Curvas Elípticas Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie-Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o ElGamal, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho. Muitos algoritmos de chave pública, como o Diffie-Hellman, o ElGamal e o Schnorr podem ser implementados em curvas elípticas sobre corpos finitos. Assim, fica resolvido um dos maiores problemas dos algoritmos de chave pública, o grande tamanho de suas chaves. Porém, os algoritmos de curvas elípticas atuais, embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA. 4. Certificado digital Com um sistema de chave pública, o gerenciamento de chaves passa a ter dois novos aspectos: primeiro, deve-se previamente localizar a chave pública de qualquer pessoa com quem se deseja comunicar e, segundo, deve-se obter uma garantia de que a chave pública encontrada seja proveniente daquela pessoa. Sem esta garantia, um intruso pode convencer os interlocutores de que chaves públicas falsas pertencem a eles. Estabelecendo um processo de confiança entre os interlocutores, o intruso pode fazer-se passar por ambos. Deste modo, quando um emissor enviar uma mensagem ao receptor solicitando sua chave pública, o intruso poderá interceptá-la e devolver-lhe uma chave pública forjada por ele. Ele também pode fazer o mesmo com o receptor, fazendo com que cada lado pense que está se comunicando com o outro, quando na verdade estão sendo interceptados pelo intruso, então este pode decifrar todas as mensagens, cifrá-las novamente ou, se preferir, até substituí-las por outras mensagens. Através deste ataque, um intruso pode causar tantos danos ou até mais do que causaria se conseguisse quebrar o algoritmo de ciframento empregado pelos interlocutores. A garantia para evitar este tipo de ataque é representada pelos certificados de chave pública, comumente chamados de certificado digital, tais certificados consistem em chaves públicas assinadas por uma pessoa de confiança. Servem para evitar tentativas de substituição de uma chave pública por outra. O certificado contém algo mais do que sua chave pública, ele apresenta informações sobre o nome, endereço e outros dados pessoais, e é assinado por alguém em quem o proprietário deposita sua confiança, uma autoridade de certificação (certification authority - CA). Assim, um certificado digital pode ser definido como um documento eletrônico, assinado digitalmente por uma terceira parte confiável. No Brasil, o órgão da autoridade certificadora raiz é o ICP-Brasil (AC-Raiz), ele é o executor das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. São autoridades certificadoras no país: Serpro (AC-SERPRO), Caixa Econômica Federal (AC-CAIXA), Serasa Experian (AC-SERASA), Receita Federal do

Brasil (AC-RFB), Certsing (AC-Certisign), Imprensa Oficial do Estado de São Paulo (AC-IOSP), Autoridade Certificadora da Justiça (AC-JUS), Autoridade Certificadora da Presidência da República (AC-PR) e Casa da Moeda do Brasil (AC-CMB). Assim, a AC-Raiz tem autoridade de emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu, sendo também encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as autoridades certificadoras (ACs) estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor. 5. Assinatura digital O sistema de criptografia assimétrica ou de chave pública também é utilizado como um meio de assinatura digital. A pessoa que assina usa sua chave privada para criptografar uma mensagem conhecida, e o texto cifrado pode ser decifrado por qualquer um usando a chave pública desta pessoa, assim como uma assinatura em papel, consiste em um bloco de informação adicionado à mensagem que comprova a identidade do emissor, confirmando quem ele diz ser. O processo se baseia em uma inversão do sistema, onde o funcionamento da assinatura digital pode ser descrito como: o emissor cifra (ou seja, atesta autenticidade) a mensagem com sua chave privada e a envia, em um processo denominado de assinatura digital. Cada um que receber a mensagem deverá verificar a validade da assinatura digital, utilizando para isso a chave pública do emissor, reconhecendo de fato, que a mensagem não foi adulterada. Como a chave pública do emissor apenas decifra (ou seja, verifica a validade) mensagens cifradas com sua chave privada, obtém-se a garantia de autenticidade, integridade e não-repudiação da mensagem, o que é apoiado pela função hashing, pois se alguém modificar um bit do conteúdo da mensagem ou se outra pessoa assiná-la ao invés do próprio emissor, o sistema de verificação não irá reconhecer a assinatura digital dele como sendo válida. É importante perceber que a assinatura digital, como descrita, não garante a confidencialidade da mensagem. Qualquer um poderá acessá-la e verificá-la, mesmo um intruso, apenas utilizando a chave pública do emissor, assim, ao empregar o uso da técnica de assinatura digital o que se busca é a garantia de autenticidade, integridade e não-repudiação da mensagem. Tabela 3 - Principais algoritmos de assinatura digital Algoritmo Descrição RSA Como já mencionado, o RSA também é comutativo e pode ser utilizado para a geração de assinatura digital. A matemática é a mesma, há uma chave pública e uma chave privada, e a segurança do sistema baseia se na dificuldade da fatoração de números grandes. ElGamal Como o RSA, o ElGamal também é comutativo, podendo ser utilizado tanto para assinatura digital quanto para gerenciamento de chaves; assim, ele obtém sua segurança da dificuldade do cálculo de logaritmos discretos em um corpo finito. DSA Inventado pela NSA e patenteado pelo governo americano, o Digital Signature Algorithm (DSA), unicamente destinado a assinaturas digitais, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão Digital Signature Standard (DSS). Adotado como padrão final em dezembro de 1994, trata de uma variação dos algoritmos de assinatura ElGamal e Schnorr. 6. Função hashing A assinatura digital obtida através do uso da criptografia assimétrica ou de chave pública infelizmente não pode ser empregada, na prática, de forma isolada, é necessário o emprego de um mecanismo fundamental para o adequado emprego da assinatura digital. Este mecanismo é a função hashing. Assim, na prática é inviável e contraproducente utilizar puramente algoritmos de chave pública para assinaturas digitais, principalmente quando se deseja assinar grandes mensagens, que podem levar preciosos minutos ou mesmo horas para serem integralmente cifradas com a chave privada de alguém, ao invés disso, é empregada uma função hashing, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, de qualquer tamanho, para oferecer agilidade nas assinaturas digitais, além de integridade confiável. Serve, portanto, para garantir a integridade do conteúdo da mensagem que representa, por isto, após o valor hash de uma mensagem ter sido calculado através do emprego de uma função hashing, qualquer modificação em seu conteúdo - mesmo em apenas um bit da mensagem - será detectada, pois um novo cálculo do valor hash sobre o conteúdo modificado resultará em um valor hash bastante distinto. Tabela 4 - Principais funções hashing Funções Descrição SHA-2 O Secure Hash Algorithm (SHA-2) por outro lado significativamente difere da função hash SHA-1, desenhado pelo NSA é uma família de duas funções hash similares, com diferentes tamanhos de bloco, conhecido como SHA-256 e SHA-512. Eles diferem no tamanho, o SHA-256 utiliza 256 bits e o SHA-512 utiliza 512 bits. Há também versões truncadas de cada padrão, conhecidos como SHA-224 e SHA-384. O ICP-Brasil em suas mudanças anunciadas adotadas para o novo padrão criptográfico do sistema de certificação digital, esta implantando em 2012, o uso do SHA-512 em substituição ao seu antecessor, o SHA-1. Um novo

padrão proposto de função de hash ainda está em desenvolvimento, pela programação do NIST a competição que apresentará esta nova função hash tem previsão de termino, com a seleção de uma função vencedora, que será dado o nome de SHA-3, ainda em 2012. SHA-1 O Secure Hash Algorithm (SHA-1), uma função de espalhamento unidirecional inventada pela NSA, gera um valor hash de 160 bits, a partir de um tamanho arbitrário de mensagem. O funcionamento interno do SHA-1 é muito parecido com o observado no MD4, indicando que os estudiosos da NSA basearam-se no MD4 e fizeram melhorias em sua segurança. De fato, a fraqueza existente em parte do MD5, descoberta após o SHA-1 ter sido proposto, não ocorre no SHA-1. Em 2005, falhas de segurança foram identificados no SHA-1, ou seja, que uma fraqueza matemática pode existir, o que indica que o uso de uma função hash mais forte é recomendável, o que motiva o uso preferencial de SHA-2. MD5 É uma função de espalhamento unidirecional inventada por Ron Rivest, do MIT, que também trabalha para a RSA Data Security. A sigla MD significa message digest. Este algoritmo produz um valor hash de 128 bits, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto em 1991, após alguns ataques de criptoanálise terem sidos descobertos contra a função hashing prévia de Rivest: a MD4. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos, e têm sido analisados pela comunidade de criptografia. Foi descoberta uma fraqueza em parte do MD5, mas até agora ela não afetou a segurança global do algoritmo. Entretanto, o fato dele produzir uma valor hash de somente 128 bits é o que causa maior preocupação; é preferível uma função hashing que produza um valor maior. MD2 e MD4 O MD4 é o precursor do MD5, tendo sido inventado por Ron Rivest. Após terem sido descobertas algumas fraquezas no MD4, Rivest escreveu o MD5. O MD4 não é mais utilizado. O MD2 é uma função de espalhamento unidirecional simplificada, e produz um hash de 128 bits. A segurança do MD2 é dependente de uma permutação aleatória de bytes. Não é recomendável sua utilização, pois, em geral, é mais lento do que as outras funções hash citadas e acredita-se que seja menos seguro. 7. Sistemas híbridos Em resumo, os algoritmos criptográficos podem ser combinados para a implementação dos três mecanismos criptográficos básicos: o ciframento, a assinatura e o hashing. Estes mecanismos são componentes dos protocolos criptográficos, embutidos na arquitetura de segurança dos produtos destinados ao comércio eletrônico. Estes protocolos criptográficos, portanto, provêm os serviços associados à criptografia que viabilizam o comércio eletrônico: disponibilidade, sigilo, controle de acesso, autenticidade, integridade e não-repúdio, usualmente apoiado por sistemas híbridos. Tabela 5 - Protocolos com Sistemas Híbridos Protocolo Descrição IPSec Padrão de protocolos criptográficos desenvolvidos para o IPv6. Realiza também o tunelamento de IP sobre IP. É composto de três mecanismos criptográficos: Authentication Header (define a função hashing para assinatura digital), Encapsulation Security Payload (define o algoritmo simétrico para ciframento) e ISAKMP (define o algoritmo assimétrico para gerência e troca de chaves de criptografia). Criptografia e tunelamento são independentes, e permite Virtual Private Network (VPN) fim-a-fim. SSL e TLS Oferecem suporte de segurança criptográfica para os protocolos NTTP, HTTP, SMTP e Telnet. Permitem utilizar diferentes algoritmos simétricos, message digest (hashing) e métodos de autenticação e gerência de chaves (assimétricos). PGP O Pretty Good Privacy (PGP), foi inventado por Phil Zimmermman em 1991, é um programa criptográfico famoso e bastante difundido na internet, destinado à criptografia de e-mail pessoal. Algoritmos suportados: hashing: MD5, SHA-1 - simétricos: CAST-128, IDEA e 3DES - assimétricos: RSA, Diffie-Hellman e DSS. S/MIME O Secure Multipurpose Internet Mail Extensions (S/MIME) consiste em um esforço de consórcio de empresas, liderado pela RSADSI e Microsoft, para adicionar segurança a mensagens eletrônicas no formato MIME. Apesar do S/MIME e PGP serem ambos padrões para a internet, o S/MIME tem sua maior utilização no mercado corporativo, enquanto o PGP é utilizado em e-mail pessoal. SET O SET é um conjunto de padrões e protocolos, para realizar transações financeiras seguras, como as realizadas com cartão de crédito na internet. Oferece um canal de comunicação seguro entre todos os envolvidos na transação. Garante autenticidade X.509v3 e privacidade entre as partes. X.509 Recomendação ITU-T, a especificação X.509 define o relacionamento entre as autoridades de certificação. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseada em nomes distintos para localização. Utilizado pelo S/MIME, IPSec, SSL/TLS e SET. Baseado em criptografia com chave pública (RSA) e assinatura digital (com hashing). 8. Conclusão Qual o modelo de criptografia que devemos utilizar, simétrico ou assimétrico? A resposta é simples, devemos utilizar os dois, em um modelo denominado híbrido. Um exemplo de combinação de emprego é encontrado ao utilizar o PGP, que combina um sistema de chave pública (Diffie-Hellmam ou

A palavra criptografia refere-se ao estudo de técnicas que a informação é transformada da sua forma original para outra forma difícil de ser identificada, ou seja, em códigos.

O termo Criptografia surgiu da fusão das palavras gregas "Kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor consiga decifrá-la. Para isso várias técnicas são usadas, e ao passar do tempo modificada, aperfeiçoada e o surgimento de novas outras de maneira que fiquem mais seguras.[8]

O principal objetivo da criptografia é que só o destinatário certo e com a chave específica possa ter acesso a determinada informação. Sendo assim, podemos defini-la também como “escrita escondida”.

2.1 - Criptografia Simétrica

RSA) com um sistema de chave privada (CAST, IDEA ou 3DES). O algoritmo simétrico, por ser muito mais rápido, é utilizado no ciframento da mensagem em si, enquanto o algoritmo assimétrico, cerca de 1.000 vezes mais lento, permite implementar a distribuição de chaves e a assinatura digital, permitindo garantir a autenticidade de quem envia a mensagem, associada à integridade do seu conteúdo, complementado com a utilização do mecanismo de hashing para assegurar a integridade da assinatura digital. Tabela 6 – Quadro comparativo Criptografia simétrica ou chave privada Criptografia assimétrica ou chave pública Rápida Lenta Gerência e distribuição das chaves é complexa Gerência e distribuição das chaves é simples Não oferece assinatura digital Oferece assinatura digital Em síntese, proteger a informação é uma máxima que persiste a cada instante quando se incrementa diariamente o número de transações comerciais e financeiras realizadas através de meios eletrônicos, em particular através da internet, neste contexto é necessário o emprego de meios e recursos para que os dados sigilosos estejam a salvo de intrusos, por isto a importância de conhecer as ferramentas e técnicas oferecidas pela criptografia, afinal desde os primórdios dos tempos o homem vem trabalhando de maneira persistente na elaboração de rotinas, que se transformaram em algoritmos poderosos, e bem empregados propiciam a proteção desejada à informação, aumentando a segurança dos dados e minimizando o impacto dos ataques submetidos às informações que trafegam através das redes de computadores, pelos seus inúmeros dispositivos conectados e muitas vezes vulneráveis. 9. Referências Bibliográficas COSTA, Celso José da e FIGUEIREDO, Luiz Manoel Silva de. Criptografia Geral. 2 ed. Rio de Janeiro : UFF / CEP - EB, 2006. 192p. – (Curso de Criptografia e Segurança em Redes). FIGUEIREDO, Luiz Manoel Silva de. Números primos e criptografia de chave pública. Rio de Janeiro : UFF / CEP - EB, 2006. 180p. – (Curso de Criptografia e Segurança em Redes – páginas 21 à 24 (31 de maio de 2012).

[8] O que é a Criptografia? www.oficinadanet.com.br/artigo/443/o_que_e_criptografia

Criptografia Simétrica: A criptografia simétrica ocorre quando o emissor e o receptor têm mesma chave de segurança capaz de traduzir a informação. É por isso que o nome é criptografia simétrica, pois a chave para criptografar e descriptografar é igual.

Este, portanto, é modelo mais antigo de criptografia, em que a chave, isto é, o elemento que dá acesso à mensagem oculta trocada entre duas partes, é igual (simétrica) para ambas as partes e deve permanecer em segredo (privada). Tipicamente, esta chave é representada por uma senha, usada tanto pelo remetente para codificar a mensagem numa ponta, como pelo destinatário para decodificá-la na outra. Essencialmente, quando a origem (ALFA) cifra uma mensagem, ele utiliza um algoritmo de ciframento para transformar o conteúdo em claro da mensagem em texto cifrado. Quando o destino (BRAVO) decifra uma mensagem, ele utiliza o algoritmo de deciframento correspondente para converter o texto cifrado de novo em uma mensagem clara. Se um intruso (CHARLIE) conhecer o algoritmo de ciframento, ele poderia decifrar uma mensagem cifrada tão facilmente quanto o destino (BRAVO). A solução no uso da criptografia de chave privada propõe que quando a origem (ALFA) cifra uma mensagem, ele utilize um algoritmo de ciframento e uma chave secreta para transformar uma mensagem clara em um texto cifrado. O destino (BRAVO), por sua vez, ao decifrar a mensagem, utiliza o algoritmo de deciframento correspondente e a mesma chave para transformar o texto cifrado em uma mensagem em claro. O intruso (CHARLIE), por não possuir a chave secreta, mesmo conhecendo o algoritmo, não conseguirá decifrar a mensagem. A segurança do sistema passa a residir não mais no algoritmo e sim na chave empregada. É ela (chave privada) que agora, no lugar do algoritmo, deverá ser mantida em segredo pela origem (ALFA) e destino (BRAVO). A principal vantagem é a simplicidade, esta técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos. Entenda que se as chaves utilizadas forem complexas a elaboração de um algoritmo de chave privada se torna bastante fácil, porém as possibilidades de interceptação são correlatas aos recursos empregados, entretanto sua utilização é considerável no processo de proteção da informação, pois quanto mais simples o algoritmo, melhor é a velocidade de processamento e facilidade de implementação. O principal problema residente na utilização deste sistema de

criptografia é que quando a chave de ciframento é a mesma utilizada para deciframento, ou esta última pode facilmente ser obtida a partir do conhecimento da primeira , ambas precisam ser compartilhadas previamente entre origem e destino , antes de se estabelecer o canal criptográfico desejado , e durante o processo de compartilhamento a senha pode ser interceptada , por isso é fundamental utilizar um canal seguro durante o compartilhamento , este independente do destinado à comunicação sigilosa , uma vez que qualquer um que tenha acesso à senha poderá descobrir o conteúdo secreto da mensagem . Outras lacunas são interpostas a este sistema : § Como cada par necessita de uma chave para se comunicar de forma segura , para um uma rede de n usuários precisaríamos de algo da ordem de n2 chaves , quantidade esta que dificulta a gerência das chaves; § A chave deve ser trocada entre as partes e armazenada de forma segura, o que nem sempre é fácil de ser garantido; § A criptografia simétrica não garante os princípios de autenticidade e não-repudiação.[9]

2.2 - Criptografia Assimétrica

Na criptografia assimétrica há duas chaves. A chave pública, que serve para criptografar as informações e a outra privada, que é utilizada para decodificar as informações.[10]

Este modelo de criptografia criado na década de 1970 - pelo matemático Clifford Cocks que trabalhava no serviço secreto inglês, o GCHQ - na qual cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública. Neste caso, as chaves não são apenas senhas, mas arquivos digitais mais complexos (que eventualmente até estão associados a uma senha). A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com

---

[9] Oliveira, Ronielton Rezende. Criptograria simétrica e assimétrica: os principais algoritmos de cifragem, Publicado na Revista online com distribuição gratuita Segurança Digital em duas partes: 5ª Edição – páginas 11 à 15 (31 de março de 2012) e 6ª Edição – páginas 21 à 24 (31 de maio de 2012).

[10] idem

outra de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular. É com a chave privada que o destinatário poderá decodificar uma mensagem que foi criptografada para ele com sua respectiva chave pública. Para entender o conceito, basta pensar num cadeado comum protegendo um determinado bem.

A mensagem é este bem, e o cadeado, que pode ficar exposto, é a chave pública.

Apenas quem tiver uma chave particular (privada) que consiga abrir o cadeado poderá acessar a mensagem. A principal vantagem deste método é a sua segurança, pois não é preciso (nem se deve) compartilhar a chave privada. Por outro lado, o tempo de processamento de mensagens com criptografia assimétrica é muitas vezes maior do que com criptografia simétrica, o que pode limitar seu uso em determinadas situações. Essencialmente, o destino (BRAVO) e todos os que desejam comunicar-se de modo seguro geram uma chave de ciframento e sua correspondente chave de deciframento. Ele mantém secreta a chave de deciframento, esta é chamada de sua chave privada. Ele torna pública a chave de ciframento, esta é chamada de sua chave pública. A chave pública realmente condiz com seu nome. Qualquer pessoa pode obter uma cópia dela.

O destino (BRAVO) inclusive encoraja isto, enviando-a para seus amigos ou publicando-a na internet. Assim, O intruso (CHARLIE) não tem nenhuma dificuldade em obtê-la. Quando a origem (ALFA) deseja enviar uma mensagem ao destino (BRAVO), precisa primeiro encontrar a chave pública dele. Feito isto, ela cifra sua mensagem utilizando a chave pública do destino (BRAVO), despachando-a em seguida. Quando o destino (BRAVO) recebe a mensagem, ele a decifra facilmente com sua chave privada. O intruso (CHARLIE), que interceptou a mensagem em trânsito, não conhece a chave privada do destino (BRAVO), embora conheça sua chave pública. Mas este conhecimento não o ajuda a decifrar a mensagem. Mesmo a origem (ALFA), que foi quem cifrou a mensagem com a chave pública do destino (BRAVO), não pode decifrá-la agora.

A grande vantagem deste sistema é permitir a qualquer um enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens. O óbice deste sistema é a complexidade empregada no desenvolvimento dos algoritmos que devem ser capazes de reconhecer a dupla de chaves existentes e poder relacionar as mesmas no momento oportuno, o que acarreta num grande poder de processamento computacional.[11]

Os smartphones utilizam a criptografia assimétrica, o que dificulta a quebra do sigilo de dados, sobretudo quando se vale de mais de um método para a desencriptação.

3 - A tecnologia *versus* a intimidade e a privacidade

Desde os primórdios a criptografia tem sido utilizada com o intuito de impedir, sobretudo, por parte do inimigo, o conhecimento de mensagens encaminhadas. O envio e o recebimento de informações sigilosas é uma necessidade antiga, que existe há centenas de anos. E daí a criptografia tornou-se uma ferramenta essencial para que apenas o emissor e o receptor tenham acesso livre às informações. O primeiro uso documentado surgiu há cerca de 1900 anos antes de cristo, no Egito, quando foram usados hieróglifos fora do padrão.[12]

Daí por diante, cada vez mais, foram se sofisticando os métodos criptográficos, culminando na famosa Enigma, criada por Arthur Scherbius, em 1918, e utilizada amplamente pelos alemães na segunda guerra, e quando foi descriptografada pelos

[11] Oliveira, Ronielton Rezende. Criptograria simétrica e assimétrica: os principais algoritmos de cifragem, Publicado na Revista online com distribuição gratuita Segurança Digital em duas partes: 5ª Edição – páginas 11 à 15 (31 de março de 2012) e 6ª Edição – páginas 21 à 24 (31 de maio de 2012).
[12] O que é Criptografia? www.oficinadanet.com.br/artigo/443/o_que_e_criptografia

aliados, segundo os historiadores, abreviou o fim da segunda grande guerra em um ano.

Com o advento da era digital, a necessidade de se guardar o sigilo de dados cresceu vertiginosamente, seja nas áreas industrial, bélica, química, etc, mas, também, no que diz respeito a intimidade e a privacidade do indivíduo, com o advento dos smartphones.

O smartphone transformou-se em um verdadeiro arquivo pessoal, onde as pessoas armazenam seus contatos, sua correspondência pessoal, suas fotografias, o caminho que percorrem, suas anotações particulares, informações que podem conter caráter de natureza íntima, inclusive de natureza sexual. A revelação de seu conteúdo pode violar a privacidade, a intimidade, violando os dados que lhe são mais caros.

Chegamos a um ponto tal onde desenvolvedores de softwares conseguem localizar pessoas através de aplicativos, mesmo quando os smartphones estão desligados, conforme se vê em uma matéria publicada pela Princeton University.

O aplicativo, denominado PinMe, extrai informações já armazenadas em smartphones que, ao contrário do GPS, não exigem permissão de acesso. Quando computados junto com mapas disponíveis publicamente e boletins meteorológicos, esses dados podem ajudar a identificar se uma pessoa está viajando a pé, de carro, de trem ou de avião e traçar sua rota de viagem.

A equipe de pesquisa informou sobre sua tecnologia de patente pendente em um artigo de 15 de setembro na revista IEEE Transactions on Multi-Scale Computing Systems.

O aplicativo, eles escreveram, usa uma série de algoritmos que localizam e rastreiam alguém processando informações como o endereço IP de um telefone e o fuso horário, junto com os dados de seus sensores. Entre outras informações, os sensores do telefone coletam detalhes da bússola a partir de um giroscópio, leituras da pressão do

ar de um barômetro e dados do acelerômetro. Todo o tempo, a presença do aplicativo pode ser praticamente indetectável.

“O PinMe demonstra como as informações de sensores aparentemente inócuos podem ser exploradas usando técnicas de aprendizado de máquina para inferir detalhes sensíveis sobre nossas vidas”, disse , professor assistente do Princeton e co-autor do artigo PinMe.

Prateek Mittal

Departamento de Engenharia Elétrica da

A precisão do PinMe tem implicações significativas em uma era de tensões aumentadas sobre as falhas de segurança e privacidade que se formam em nossas vidas cada vez mais digitalizadas. Os criadores do PinMe esperam que a exposição da falha de segurança do sensor influencie a próxima geração de sistemas operacionais para smartphones a incluir um switch "off" para dados de sensores, alguns dos quais coletados para aplicativos de fitness e jogos interativos que rastreiam os movimentos das pessoas.

"Queríamos aumentar a preocupação pública sobre esse assunto", disse Arsalan Mosenia, pesquisador de pós-doutorado em engenharia elétrica e membro da equipe da PinMe.

Apesar das conclusões preocupantes, as consequências do PinMe não são todas sinistras, dizem os desenvolvedores. A tecnologia é uma forte alternativa à navegação baseada em GPS em carros autônomos e outras formas de transporte, já que os sinais de GPS são suscetíveis a fraudes.

"Os atacantes podem convencer um navio ou carro de que estão em um local em que não estão", o que pode ser problemático para navios americanos que navegam em águas internacionais, por exemplo, ou para a segurança de passageiros de carros autônomos aponta , professor de engenharia elétrica em Princeton e co-autor do artigo. A equipe do PinMe já está conversando com empresas de tecnologia sobre o licenciamento do aplicativo como uma ferramenta de navegação.

Niraj Jha

Mosenia desenvolveu o aplicativo no ano passado como um estudante de Ph.D em Princeton, em colaboração com Mittal, Jha e Xiaoliang Dai, Ph.D. em Engenharia Elétrica de Princeton.

A equipe tentou empurrar os limites de pesquisas anteriores sobre a segurança do telefone, disse Mosenia. Outros cientistas usaram dados de sensores para localizar pessoas medindo o consumo de energia de telefones enquanto viajam por ruas conhecidas ou lendo o acelerômetro.

Mas seus aplicativos só podiam lidar com um modo de viagem, geralmente dirigindo, e precisavam de informações antecipadas sobre o proprietário do telefone, como a localização inicial ou a área em que a pessoa estava viajando. Alguns aplicativos também coletavam dados com tanta frequência, até 40 hertz ou 40 vezes por segundo, que eram obrigados a levantar a suspeita de aplicativos de segurança.

O que torna o PinMe tão poderoso e, portanto, indetectável, é que ele precisa apenas coletar um drible de dados: cinco vezes por segundo, em média (para dirigir, a taxa é ainda menor: uma vez a cada 10 segundos). Também pode rastrear uma pessoa através de múltiplos modos de viagem e não precisa de informações antecipadas.

"Para realizar o experimento, os pesquisadores de Princeton coletaram dados do telefone de três pessoas por um dia após a instalação do PinMe em seus telefones - Galaxy S4 i9500, iPhone 6 e iPhone 6S - rodando Android ou iOS. Os sujeitos do estudo viajaram a pé, de carro, de trem e de avião por cidades como Filadélfia, Dallas e Princeton.

O PinMe primeiro leu o último endereço IP e o status de rede de cada telefone para encontrar sua última conexão Wi-Fi. Isso reduziu a pesquisa, expondo a localização mais recente do telefone.

Em seguida, para determinar o modo de viagem, o aplicativo usava um algoritmo de aprendizado de máquina que havia sido treinado para reconhecer a diferença entre caminhar, dirigir, andar de trem e voar. Isso foi feito reunindo pistas dos sensores de um telefone que expunham informações cruciais: a rapidez com que a pessoa se movia e a direção da viagem, com que freqüência a pessoa estava parando e depois se movimentando de novo e a altitude da pessoa.

Uma vez que a atividade da pessoa foi revelada, o PinMe lançou um dos quatro algoritmos adicionais direcionados para cada meio de transporte. Esses cálculos mapearam a rota pela qual a pessoa estava viajando, combinando dados do telefone com informações públicas. Mapas de navegação disponíveis a partir do software open-source OpenStreetMap, por exemplo, ajudaram o PinMe a mapear as rotas de viagem específicas do telefone, enquanto os mapas de altitude do Google e do US Geological Survey ofereciam detalhes de altitude para cada ponto da Terra.

O aplicativo também usou relatórios detalhados de temperatura, umidade e pressão de ar das várias estações meteorológicas do The Weather Channel para contextualizar as leituras do sensor de pressão de ar de um telefone, já que elas são influenciadas pelas condições climáticas e pela altitude. Horários de trens e aviões também ofereciam pistas.

Quando um sujeito de teste voou da Filadélfia para Dallas, por exemplo, o aplicativo reconheceu picos de elevação e aceleração. Isso implicava que a pessoa estava em um avião que estava decolando ou pousando. O lapso de tempo entre os picos revelou a duração do voo. Em seguida, as provas, incluindo os dados do fuso horário, em combinação com os níveis climáticos e de elevação dos aeroportos, além dos horários dos vôos, foram combinados para identificar corretamente os aeroportos de decolagem e pouso.

Embora o PinMe seja extremamente preciso para muitos modos de viagem, não é perfeito. Um software como o Tor, que pode ser instalado para ocultar endereços IP de

rastreadores, tornaria o telefone difícil, embora não impossível, de identificar. O PinMe também poderia vacilar com a mineração de registros públicos ruins, ou seguindo alguém por uma cidade, como Manhattan, sem mudanças de elevação e estradas parecidas com o meio-ambiente em uma grade.

No futuro, as pessoas poderão desativar seus sensores. Mas por enquanto, sem desligar o telefone, há pouca esperança de se esconder do PinMe, que é uma grande preocupação para especialistas em segurança de dados, como Supriyo Chakraborty, pesquisador do Centro de Pesquisa Thomas J. Watson da IBM.

"O ataque [PinMe] é ... extremamente potente", disse Chakraborty, que não estava envolvido na pesquisa.

Os desenvolvedores da PinMe já estão trabalhando em maneiras de as pessoas se defenderem, disse Jha, cujo foco de pesquisa é a segurança da “internet das coisas”, uma frase que descreve os produtos cada vez mais digitais que impulsionam nossas atividades diárias.

"Acho que muito acompanhamento deve lidar com a forma de evitar este ataque", disse ele.[13]

Isto, por si só, já demonstra a fragilidade, que os usuários de smartphones estão submetidos, em face da popularização e da disponibilidade cada vez maior da tecnologia posta a disposição do cidadão comum.

No Brasil foi publicada em 15 de agosto de 2018 a Lei geral sobre a proteção de dados pessoais (Lei nº 13.709/2018), que entrará em vigor a partir de 15 de janeiro de 2020.

---

[13] Shekhtman, Lonnie - Telefones vulneráveis ao rastreamento de localização, mesmo quando o GPS está desativado - www.princeton.edu/news/2017/11/29/phones-vulnerable-location-tracking-even-when-gps-services

Essa Lei traz regras para disciplinar a forma como os dados pessoais dos indivíduos podem ser armazenados por empresas ou mesmo por outras pessoas físicas.

O objetivo da Lei é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A Lei nº 13.709/2018 utiliza, em diversos momentos, a expressão “tratamento de dados pessoais”. O que quer dizer essa expressão?

Tratamento de dados pessoais é toda “operação” realizada com dados pessoais.

Tratamento de dados pessoais, portanto, é toda e qualquer operação realizada com dados pessoais. Isso inclui toda e qualquer conduta realizada com dados pessoais. Exs: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão e extração.

O grande objetivo da Lei nº 13.709/2018, portanto, é esse: estabelecer regras sobre como as empresas e o poder público tratam os dados pessoais, ou seja, como coletam, como armazenam, como vendem etc., fixando limites para que isso ocorra.

Esta Lei se aplica a qualquer operação de tratamento de dados pessoais...
- Realizada por pessoa natural ou por pessoa jurídica de direito público ou privado
- Independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
• os dados pessoais tenham sido coletados no Brasil ou qualquer outra operação de tratamento seja realizada em nosso país. Ex: a pesquisa no supermercado.
• a atividade de tratamento tenha sido feita fora do Brasil, mas ela tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional. Ex: cadastro no Facebook ou em outros sites estrangeiros, mas que utilizem esses dados para vender produtos aqui no Brasil.

No entanto, a lei supra referida, na forma de seu artigo 4º, III, não se aplica:

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais.[14]

4 - Do direito à vida privada

Nos Estados Unidos, como em geral nos países de língua inglesa, utiliza-se a expressão privacy (“privacidade”), em right to/of privacy, para indicar pretensões jurídicas de ver respeitada a esfera de autonomia pessoal e familiar, especialmente quanto: a) ao direito de ser deixado em paz (tort privacy) – não se admitindo a obtenção e disseminação não autorizadas de informações pessoais.

A revelação de assuntos privados é tanto mais séria quanto mais exponha o indivíduo aos olhos do público de uma forma capaz de incriminá-lo, sobretudo, quando há, apreensão de bens e objetos pessoais (fourth amendment privacy) realizadas na esfera privada.

No direito europeu, a expressão empregada é o “direito ao respeito da vida privada”, cujo objeto inclui o respeito à inviolabilidade da correspondência, reunindo a liberdade e a inviolabilidade das comunicações em geral; além da garantia de intangibilidade do domicílio, igualmente desdobrada em seu aspecto passivo, de inviolabilidade, e ativo,

[14] www.dizerodireito.com.br/2018/08/lei-137092018-lei-geral-de-protecao-de.html

de autonomia; associados a um regime de proteção aos dados pessoais e à liberdade e identidade sexual e da vida familiar.

Na literatura alemã, encontramos diferentes nomes para distintos extratos de atuação da vida individual: íntimo, secreto, privado, social e público, bem como uma recente elaboração de um informationelle Selbstbestimmungsrecht (direito de autodeterminação informacional), extraídos, a partir de um juízo concreto de ponderação, do "direito geral da personalidade" (elemento passivo do desenvolvimento da personalidade: referência à situação do "ser") e do "direito geral de liberdade" (elemento ativo daquele desenvolvimento: referência à ação, ao "fazer") assegurados pelos arts. 1.1 e 2.1 da Lei Fundamental de Bonn. O "direito geral da personalidade", para alguns, considerado como uma parte da teoria das esferas elevada ao nível dos direitos, é precisado a partir da efetivação de direitos mais concretos, tais como: a) o direito às esferas íntima, secreta e privada, assegurando o respeito de um "âmbito protegido" e de uma situação de inviolabilidade documental, de dados e de comunicações pessoais, sendo a intimidade o núcleo mais sensível e, consequentemente, nuclear da esfera privada, "espaço último intangível da liberdade humana" (BVerfGE 6, 32 (41)), em que o indivíduo, por não afetar, por meio de seu "ser" ou de seus comportamentos, a esfera pessoal dos congêneres ou o interesse da vida da comunidade" (BVerfGE 35, 202 (220)), exige uma proteção maior relativamente à esfera privada, em que essa afetação se faz presente e a ação intersubjetiva se opera de forma mais contundente. No âmbito dessa proteção se incluem a honra e o prestígio social, a identidade, a própria imagem e a voz, mais a liberdade profissional; b) direitos de autodeterminação, designadamente sexual e informacional, esta com a tendência a sobrepor-se à teoria das esferas. Na França, o art. 9º do Código Civil diferencia o direito ao respeito da vida privada, consagrado em sua primeira parte, da intimidade da vida privada, prevista na sua segunda parte, hábil esta a autorizar a adoção de medidas judiciais vigorosas como o sequestro e a busca e apreensão da matéria jornalística portadora de une atteinte intolérable à personnalité. Fala-se assim de uma "vida privada íntima" e de uma "vida privada ordinária", cujos atentados importam distintas consequências jurídicas: sequestros, buscas e apreensões, responsabilidade civil, no primeiro caso; apenas

demanda indenizatória, no segundo. O significado de “intimidade da vida privada” tem sido dado pelos tribunais: seriam aquelas intromissões intoleráveis, de captação e divulgação de informações pessoais, como o estado de saúde, a realização de cirurgias, a vida amorosa e sentimental de alguém. Nos países de língua espanhola, domina o entendimento de que intimidade e vida privada, embora possam ter, em abstrato, conceitos distintos, operacionalmente não revelam desigualdade significativa, podendo, conseguintemente, ser usados ambos os termos para designar o mesmo recorte jurídico, enfim, a mesma coisa. No Brasil há uma tendência nesse mesmo sentido. Usam-se intimidade e vida privada indistintamente, embora alguns ressaltem ser aquela um extrato mais restrito desta. Sem embargo de seus respeitáveis defensores, há que se fazer radical distinção a partir das lições do direito comparado e mesmo da matriz etimológica das duas expressões, sem esquecer ainda do fator de diferenciação feito pela disposição constitucional consagradora de um geral direito à vida privada e à intimidade: “são invioláveis a intimidade, a vida privada...” (art. 5º, X, da CF). Ou, se quisermos maior distinção, direitos da esfera privada. O direito geral à vida privada (ou direitos da esfera privada) desafia uma compreensão muito mais ampla, assentada na própria ideia de autonomia privada e da noção de livre desenvolvimento da personalidade, sem embargo, contida em certos desdobramentos materializantes, como a seguir veremos. Tais desdobramentos são produto de uma dada realidade social, econômica e política, percebível pelo pensamento jurídico contemporâneo e, por ele, revelado. Essa materialização, por outro lado, não se expande a domínios indefinidos, nem contempla todas as potencialidades e mesmo manipulações ideológicas da “autonomia privada”, circunscrevendo-se antes a um âmbito da existencialidade humana e suas projeções mais acercas. [15]

[15] STJ. No que concerne à ilegalidade das provas colhidas no aparelho telefônico do recorrente, tem- se que, a despeito de a situação retratada não se configurar como interceptação telefônica de comunicações, demanda igualmente autorização judicial devidamente motivada — haja vista a garantia constitucional à intimidade e à vida privada —, o que efetivamente foi observado no caso dos autos. De fato, o celular do recorrente foi apreendido em razão de mandado de busca e apreensão, devidamente fundamentado, que autorizou a apreensão de aparelhos eletrônicos, bem como o acesso às informações armazenadas, desde que guardem relação com o crime sob investigação. 5. Recurso em habeas corpus improvido. (RHC 64.713/SP - Rei. Min. Reynaldo Soares da Fonseca - DJe 02.12.2016). TJRJ: É certo que o art. 6o do Código de Processo Penal, em seus incisos II e III, determina a apreensão de objetos e a colheita de provas logo que a autoridade policial tomar conhecimento da prática de infração penal. 2. Ocorre que, in casu, a despeito de denúncia anônima, nada de ilícito foi encontrado em poder dos acusados “o que se faz concluir que não havia indício suficientemente hígido acerca da prática de infração penal" não estando

Tudo porque conjuga os sentidos de “autonomia”, “personalidade” e “dignidade humana” sob uma metodologia jurídica de pesquisa e argumentação que o substancializa, dando-lhe cores e fronteiras. Sem qualquer pretensão de esgotar o conteúdo do direito à vida privada, porém atentos às lições do direito comparado, podemos apresentar os seguintes componentes definidores desse conteúdo: a liberdade sexual; a liberdade da vida familiar; a intimidade; além de outros aspectos de intercessão com demais bens ou atributos da personalidade.[16]

A Procuradoria Geral da República Portuguesa assim se manifesta em parte do seu parecer n.º 95/2003 - Direito à imagem - Direito a informar - Recolha de imagem - Intimidade da vida privada - Direitos, liberdades e garantias - Conflito de direitos - Fotografia ilícita - Medida de polícia Devassa da vida privada.[17]

---

autorizada, portanto, a apreensão de objetos de posse lícita sem a autorização de seus respectivos proprietários. 3. Muito menos está autorizado, com fulcro na norma do art. 6o em comento, o acesso às informações contidas nos telefones celulares de quaisquer indivíduos, tampouco a oitiva desautorizada e forçada de suas respectivas conversas telefônicas, o que viola a norma do art. 5 , incisos X e XII, da Constituição Republicana, que asseguram, como direito fundamental, a inviolabilidade da intimidade e a inviolabilidade do sigilo das comunicações telefônicas. 4. Por conseguinte, as provas obtidas por meio da ingerência policial na intimidade, na vida privada e nas comunicações telefônicas, sem observância das exigências legais e constitucionais se revelam flagrantemente ilícitas, devendo ser desentranha- j das dos autos. Art. 157 do Código de Processo Penal e art. 5o, inc. LVI, | da Constituição Republicana... (TJ-RJ — APL: 00231663620138190023 | - Rei. Paulo de Oliveira Lanzellotti Baldez)

[16] Canotilho, J,J, Comentários à Constituição do Brasil / J. J. Gomes Canotilho...[et al.] ; outros autores e coordenadores Ingo Wolfgang Sarlet, Lenio Luiz Streck, Gilmar Ferreira Mendes. – 2. ed. – São Paulo : Saraiva Educação, 2018.

[17] 1 Quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual:
a) Interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa ou comunicação telefónica;
b) Captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objectos ou espaços íntimos;
c) Observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou
d) Divulgar factos relativos à vida privada ou a doença grave de outra pessoa; é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.
2 – O facto previsto na alínea d) do número anterior não é punível quando for praticado como meio adequado para realizar um interesse público legítimo e relevante."
Segundo Costa Andrade (ver nota 35), "[a] justificação a título de prossecução de interesses legítimos pressupõe ainda o respeito das exigências da idoneidade, proporcionalidade e necessidade.
Neste contexto, assume relevo o chamado direito ao anonimato, que se opõe à identificação da pessoa concretamente atingida (através, v. g., da publicação do nome) sempre que tal não seja necessário à satisfação dos interesses a prosseguir. É o que, em princípio, poderá adiantar-se para as hipóteses em que não estejam em causa pessoas da história do tempo, ou acontecimentos de inequívoco significado comunitário. Quando, por exemplo, a imprensa pode satisfazer o interesse da comunidade sem identificar ou tornar inequivocamente reconhecível aquele sobre quem são divulgados os factos [...], então a publicação do nome, da fotografia ou a individualização por outro processo ultrapassa a barreira da necessidade ".

E, mais adiante, prossegue o mesmo autor, no citado Comentário Conimbricense do Código Penal, "[o] que fica dito vale sobremaneira para a divulgação de factos criminosos. Configurando um evento de inequívoco relevo comunitário, o crime não pertence à área de reserva, sendo, por isso, objecto legítimo de investigação e notícia, nomeadamente através da imprensa (jornais, rádio, televisão, etc.). Que devem agir com o respeito possível pelo princípio de presunção de inocência e pelo direito à ressocialização do condenado".

Os órgãos da comunicação social figuram entre os destinatários privilegiados da justificação a coberto da prossecução de interesses legítimos. "Que podem reivindicar da prossecução de interesses públicos, legítimos e relevantes sempre que actuam no âmbito da função pública da imprensa. 'Onde cabe toda a sua actividade relativa à formação democrática e pluralista da opinião pública em matéria social, política, económica e cultural' (Figueiredo Dias, Revista de Legislação e de Jurisprudência, ano 115.º, p. 136). Já o mesmo não valerá para a procura do escândalo ou o cultivo do sensacionalismo. Claro que os media podem cultivar legitimamente o sensacionalismo e o escândalo (com vista designadamente à maximização das tiragens), desde que o façam sem afronta às normas penais. Isto porquanto a procura do sensacionalismo e do escândalo não pode valer como referente teleológico indispensável para os efeitos de justificação de atentados típicos contra a vida privada.".

O procedimento criminal pelo crime de devassa da vida privada depende de queixa, nos termos do estatuído no artigo 198.º do Código Penal.

3 Na ordem jurídica portuguesa, o direito à imagem (ver nota 37) constitui um direito autónomo (distinto da privacidade), encontrando-se protegido constitucionalmente, a par de outros direitos de personalidade, no citado n.º 1 do artigo 26.º da Constituição. De acordo com Gomes Canotilho e Vital Moreira (ver nota 38), o direito à imagem abrange não só o direito de cada um de não ser fotografado nem ver o seu retrato exposto em público sem seu consentimento mas também o direito de não o ver apresentado em forma gráfica ou montagem ofensiva e malevolamente distorcida ou infiel.

"O direito à imagem é o mais exterior e público dos direitos da pessoa (física) e, destarte, é o que é mais susceptível de ser ofendido."

Com efeito, fora da esfera íntima da sua vida privada, a pessoa física encontra-se permanentemente exposta ao exame do público.

Na lição de Adriano de Cupis, "a necessidade de proteger a pessoa contra a arbitrária difusão da sua imagem, deriva de uma exigência individualista, segundo a qual a pessoa deve ser árbitro de consentir ou não na reprodução das suas próprias feições: o sentido cioso da própria individualidade cria uma exigência de circunspecção, de reserva. A referida necessidade tornou se mais forte com os progressos técnicos, que permitiram o emprego do processo fotográfico, o qual facilita muito a reprodução [] A exigência social dirigida ao conhecimento e à crítica dos indivíduos e dos factos privados actua em sentido oposto []." Ora, por força do disposto no n.º 1 do artigo 79.º do Código Civil, o retrato de uma pessoa não pode ser exposto ou publicado sem o seu consentimento.

O citado artigo 79.º estabelece:

"Artigo 79.º

Direito à imagem

O retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem consentimento dela; depois da morte da pessoa retratada, a autorização compete às pessoas designadas no n.º 2 do artigo 71.º, segundo a ordem nele indicada.

Não é necessário o consentimento da pessoa retratada quando assim o justifique a sua notoriedade, o cargo que desempenhe, exigências de polícia ou de justiça, finalidades científicas, didácticas ou culturais, ou quando a reprodução da imagem vier enquadrada na de lugares públicos, ou na de factos de interesse público ou que hajam decorrido publicamente.

O retrato não pode, porém, ser reproduzido, exposto ou lançado no comércio se do facto resultar prejuízo para a honra, reputação ou simples decoro da pessoa retratada."

Portanto, atenta a letra da lei, o ordenamento juscivilista apenas considera ilegítima a exposição, reprodução ou comercialização do retrato, mas não a simples fixação da imagem num retrato.

"No que respeita a pessoas revestidas de notoriedade, a lei entendeu satisfazer o interesse do público em conhecer a sua imagem. Trata-se de casos determinados, nos quais a exigência social, dirigida ao conhecimento da imagem da pessoa, é particularmente sensível, devendo, em tais casos, o direito à imagem ceder em face dela. De qualquer modo, mesmo as pessoas revestidas de notoriedade

conservam o direito à imagem relativamente à esfera íntima da sua vida privada, em face da qual as exigências de curiosidade pública têm de deter-se.".

O cargo público exercido é incluído pela lei entre os casos de limitação legal do direito à imagem, já que o interesse público em conhecer a imagem dos respectivos titulares sobreleva, nessas hipóteses, o interesse privado.

Efetivamente, "[o] interesse da sociedade estende-se sobre todos os que desempenham uma função pública de notável importância e que são
rodeados, a tal título, de notoriedade. As necessidades da justiça ou de polícia, os fins científicos, didácticos ou culturais, constituem outras
tantas hipóteses especificamente determinadas, nas quais o sentido da individualidade deve ceder em face de exigências opostas de carácter
geral. O mesmo sentido da individualidade deve, do mesmo modo, ceder quando a reprodução esteja ligada a factos, acontecimentos ou
cerimónias de interesse público ou realizadas em público."(ver nota 43).

A protecção de forma autónoma e individualizada do direito à imagem está penalmente tutelada no capítulo VIII ("Dos crimes contra outros bens jurídicos") do título I ("Dos crimes contra as pessoas") do livro II ("Parte especial") do Código Penal.

Dispõe, a este respeito, o artigo 199.º do Código Penal:

"Artigo 199.º

Gravações e fotografias ilícitas

1 Quem, sem consentimento:

a) Gravar palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas; ou

b) Utilizar ou permitir que se utilizem as gravações referidas na alínea anterior, mesmo que licitamente produzidas;

é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.

2 Na mesma pena incorre quem, contra vontade:

a) Fotografar ou filmar outra pessoa, mesmo em eventos em que tenha legitimamente participado; ou

b) Utilizar ou permitir que se utilizem fotografias ou filmes referidos na alínea anterior, mesmo que licitamente obtidos.

3 É correspondentemente aplicável o disposto nos artigos 197.º e 198.º"

O texto do artigo transcrito resulta da revisão do Código Penal operada pelo DecretoLei
n.º 48/95, de 15 de Março ..

Os trabalhos preparatórios e a discussão parlamentar que antecedeu a concessão ao Governo de autorização legislativa para rever o Código Penal fornecem contributos para o tratamento do tema que nos ocupa. O deputado Costa Andrade (PSD), intervindo na reunião da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias com representantes do Sindicato de Jornalistas, que teve lugar em 25 de Maio de 1994 e em 14 de Junho seguinte, afirmou:

"[...] não podemos esquecer aqui o Código Civil, que alarga as justificações, designadamente em relação às fotografias e filmes, porque diz que não são ilícitas as fotografias feitas de pessoas notáveis, para fins didácticos e científicos, em lugares e eventos públicos. Ora, é óbvio que todas essas justificações do Código Civil valem, por força do princípio da subsidiariedade do direito penal, e, portanto, não pode ser penalmente ilícito aquilo que é lícito segundo outro ramo do direito

Assim, digamos relativamente ao crime de fotografias ilícitas, se conjugarmos o artigo do Código Penal com o do Código Civil, a incriminação estreita, quase tendencialmente, até à fotografia íntima. Se projectarmos bem o regime do Código Civil sobre o universo de casos em abstracto típicos segundo a incriminação do Código Penal, aquele deixa uma margem extremamente escassa de fotografia ilícita, porque exclui a incriminação quando se fotografa com fins científicos, didácticos, em lugares e manifestações públicas, etc.

Penso, portanto, que um jornalista pode fotografar tudo o que diz respeito ao público, mas já tenho dúvidas que outras instâncias, que não os jornalistas, o possam fazer ou, pelo menos, que o possam fazer individualizando pessoas."E mais adiante prosseguiu:

"[...] quanto às fotografias ilícitas, as alterações ao Código Penal, na medida em que existem e são poucas resultam em estreitar o âmbito punível. Quer dizer, a fotografia resultará menos punível com

estas alterações do que com o direito vigente. Porque se faz depender a licitude ou ilicitude da fotografia de ser contra a vontade da pessoa enquanto que, actualmente, é sem consentimento de quem de direito. Uma coisa é fazer algo sem consentimento, outra é ir contra a vontade, o que significa que a pessoa em causa se pronunciou.
Para além disso que vale, obviamente, em direito penal , não podemos esquecer a justificação das fotografias ilícitas inserida no Código Civil.
O Código Civil tem um artigo sobre fotografias que diz mais ou menos que são lícitas as fotografias em lugares públicos, para fins científicos, etc. Em termos tais que, se combinarmos, como temos sempre de fazer (para um jornalista, isto pode não ser claro, mas, para um jornalista jurista, é obviamente claro), o Código Penal com o Código Civil uma vez que, por força do artigo 31.º do Código Penal, todas as causas de justificação existentes em qualquer ramo da ordem jurídica valem em direito penal (o direito penal não pode declarar ilícito aquilo que qualquer ramo do direito declara lícito) para as fotografias penalmente ilícitas, como tal, sobra relativamente pouco.
No fundo, resultará criminalizável a fotografia que já o seria em nome da intimidade e não da imagem.".
Por seu turno, a deputada Odete Santos (PCP), intervindo no debate, na generalidade, da proposta de lei n.º 92/VI, sustentou (ver nota 49):
"Na avaliação das alterações que se introduziram a alguns tipos de crimes, eliminando a expressão 'sem justa causa', que para uns constitui uma menção redundante da ilicitude, e para outros integra a própria factualidade do tipo, quanto ao crime das gravações e fotografias ilícitas, registamos que, a propósito da expressão 'sem justa causa', alguma doutrina conclui que há uma 'extensão acrescida da incriminação'.
Ponderados os interesses em conflito o das vítimas e os daqueles que exercem o direito de informar , parece-nos que, apesar de a parte geral do Código poder resolver o problema, se deve entender como útil, como diz a doutrina alemã, que as normas incriminatórias advirtam que ocorrem muitas vezes situações de conflito que reclamam a justificação da conduta, apesar do preenchimento do tipo."
Conforme salienta Costa Andrade (ver nota 50), "[n]a determinação da área de tutela típica do direito à imagem deve ainda ter-se presente o disposto no n.º 2 do artigo 79.º do Código Civil. Que, pelo menos em algumas constelações previstas, se projecta em sede de tipicidade e não apenas de ilicitude/justificação. Deve ser assim em relação a dois grupos de casos: a) [e]m primeiro lugar [...], quando a 'imagem vier enquadrada na de lugares públicos ou na de factos de interesse público ou hajam decorrido publicamente'. Isto na medida em que a imagem da pessoa resulte inequivocamente integrada na 'imagem' daqueles espaços ou eventos e neles se dissolva [...]; b) [e]m segundo lugar, quando
seja relevante a 'notoriedade ou o cargo desempenhado'. Num caso e noutro a exclusão da responsabilidade criminal actualiza-se logo em sede de tipicidade []".
Por outro lado, quanto à eliminação do inciso "justa causa" como excludente da responsabilidade penal, o mesmo autor aponta duas razões decisivas que pesaram na decisão do legislador de 1995: "[e]m primeiro lugar, as controvérsias quanto à natureza da figura: autêntica (e autónoma) causa de justificação ou mera menção redundante da ilicitude? (cf. Figueiredo Dias, O Problema, pp. 447 e segs.); [e]m segundo lugar e sobretudo, a circunstância de, à vista do largo espectro de dirimentes da ilicitude consignadas na lei penal portuguesa, não ter sido possível referenciar qualquer margem de justificação autónoma a título de justa causa. Brevitatis causa: o legislador de 1995 entendeu que o inciso sem causa justa deveria ser levado à conta de manifestação arquetípica da menção redundante da ilicitude".
Nesta perspectiva, "a interpretação da incriminação das fotografias ilícitas constante do Código Penal terá sempre de actualizar-se em integração sistemática com a ordem jurídica no seu conjunto. É o que impõe o postulado da unidade do sistema jurídico (artigo 31.º do Código Penal): que afasta sem mais o estigma da ilicitude penal em relação a condutas autorizadas ou legitimadas por força de qualquer outro ramo do ordenamento jurídico".
O procedimento criminal respeitante ao crime de gravações e fotografias ilícitas depende de queixa, por força das disposições combinadas do n.º 3 do artigo 199.º e do artigo 198.º, ambos do Código Penal, sendo titular da queixa a pessoa cuja imagem foi captada ou utilizada (artigo 113.º do Código Penal), pelo que é necessária a denúncia do facto pelos titulares do direito de queixa para que o Ministério Público possa promover o processo penal (artigos 48.º, 49.º e 241.º a 247.º, todos do Código de Processo Penal).

A questão de fundo que emerge da análise da relação entre o direito de informação e os direitos pessoais ou da personalidade é a difícil compatibilização entre o primado do social, que é inerente à comunicação social, e o primado da dignidade humana, que é reclamado pela afirmação dos direitos humanos.
Efectivamente, são quotidianos os casos de conflito entre o direito de informação e os direitos pessoais, como sejam o direito ao bom nome e reputação, à imagem e à reserva da intimidade da vida privada e familiar .
A ideia básica proposta pela doutrina (ver nota 55) e aceite pela jurisprudência (ver nota 56) para a resolução concreta destes conflitos é a da harmonização ou da concordância prática.
Os direitos fundamentais enunciados revestem a natureza de direitos, liberdades e garantias, pelo que, todos eles, estão submetidos ao regime específico estabelecido na Constituição para esta categoria de direitos.
Assim, a resolução de eventuais conflitos entre esses direitos tem de realizar-se luz do direito constitucional .
Assim, a resolução de eventuais conflitos entre esses direitos tem de realizar-se à luz do direito constitucional . "Nesse regime destaca-se, do ponto de vista material ou substancial, o carácter de direito directamente aplicável e o facto de tais direitos não poderem ser restringidos senão nos casos expressamente admitidos pela Constituição (artigo 18.º, n.º 2). Por outro lado, a intervenção restritiva, mesmo que constitucionalmente autorizada, somente será legítima se justificada pela salvaguarda de outro direito fundamental ou de outro interesse constitucionalmente protegido (artigo 18.º, n.º 2). Finalmente, as leis restritivas, além do carácter geral e abstracto, têm de respeitar, em qualquer caso, o princípio da proporcionalidade e o conteúdo essencial dos direitos (artigo 18.º, n.os 2 e 3). Na perspectiva orgânica, é de salientar que as restrições estão sujeitas a reserva de lei, apenas sendo legítimas as intervenções da autoria da Assembleia da República ou do Governo se munido de credencial parlamentar (artigo 18.º, n.º 2, da CRP).
Do regime exposto, importa sublinhar que os direitos, liberdades e garantias só podem ser restringidos nos casos expressamente previstos na própria Constituição, compreendendo-se nesta asserção as restrições constitucionalmente expressas, as estabelecidas por lei com autorização da Constituição e o caso dos 'limites imanentes' .
Na verdade, nenhum direito pode ser entendido com um alcance absoluto. Sempre que um direito conflitue com outro direito ou bens constitucionalmente protegidos, esse conflito deve ser resolvido através da recíproca e proporcional limitação de ambos, em ordem a optimizar a solução (princípio da concordância prática) de modo a garantir uma relação de convivência equilibrada e harmónica em toda a medida possível.
Por conseguinte, além de precisarem de credencial constitucional, as restrições de direitos fundamentais carecem também de justificação, sendo apenas legítimas as impostas pela necessidade de salvaguardar outros direitos ou interesses constitucionalmente protegidos.
Finalmente, a medida restritiva estabelecida por lei tem de respeitar o princípio da proporcionalidade nas suas três dimensões (artigo 18.º, n.º2).
O princípio da proporcionalidade ou da proibição do excesso segundo a terminologia da doutrina alemã que se desdobra em três corolários ou subprincípios: o da conformidade ou adequação, o da exigibilidade ou necessidade e o da justa medida ou da proporcionalidade em sentido estrito.
O subprincípio da conformidade ou adequação (idoneidade) impõe que a medida adoptada para a realização do interesse público deva ser apropriada à prossecução do fim público subjacente. Tal imposição exige a investigação e a prova de que o acto do poder público é idóneo para a concretização dos fins justificativos da sua adopção. Trata-se, por conseguinte, de controlar a relação de adequação medida fim.
O subprincípio da exigibilidade ou necessidade (ver nota x6), partindo da ideia de que o cidadão tem direito à menor desvantagem possível, impõe, na escolha entre os meios abstractamente idóneos à consecução do objectivo prefixado, aquele cuja adopção implique as consequências menos negativas para os privados. Além de idóneo exegese que o meio escolhido seja necessário. Para esse efeito impõe se provar sempre que, para a obtenção de determinados fins, não era possível adoptar outro meio menos oneroso para o cidadão.

4.1 - Da inviolabilidade do sigilo de dados

No dizer de Tercio Sampaio Ferraz Jr “O sigilo de dados é uma hipótese nova, trazida pela Constituição Federal de 1988. A inovação trouxe com ela dúvidas interpretativas que merecem, por isso mesmo, uma reflexão mais detida.

A inviolabilidade do sigilo de dados (art.5° — XII) é correlata ao direito fundamental à privacidade (art. 5° — X). Em questão está o direito de o indivíduo excluir do conhecimento de terceiros aquilo que a ele só é pertinente e que diz respeito ao seu modo de ser exclusivo no âmbito de sua vida privada. Mister se faz, pois, explicitar a correlação entre sigilo e privacidade, assinalando também o que os distingue. Principiemos com o direito à privacidade.

Trata-se de um direito subjetivo fundamental. Como direito subjetivo, manifesta uma estrutura básica, cujos elementos são o sujeito, o conteúdo e o objeto. O sujeito é o titular do direito. Em se tratando de um dos direitos fundamentais do indivíduo, o sujeito é todo e qualquer pessoa, física ou jurídica, brasileira ou estrangeira, residente (ou transeunte — cf. Mello Filho, 1984:20) no país (art. 5°, caput).

O conteúdo é a faculdade específica atribuída ao sujeito, que pode ser a faculdade de constranger os outros ou de resistir-lhes (caso dos direitos pessoais) ou de dispor, gozar, usufruir (caso dos direitos reais). A privacidade, como direito, tem por conteúdo a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é,

---

Por último, o subprincípio da justa medida ou proporcionalidade em sentido estrito postula um juízo de ponderação com vista a impedir a adopção de medidas excessivas ou desproporcionadas para alcançar os fins pretendidos, devendo pesar-lhe as desvantagens dos meios em relação às vantagens do fim ."

3 No contexto da matéria a que se refere a consulta, para além da tarefa de ponderação e harmonização concretas entre o direito de informação e os direitos pessoais à reserva da vida privada, à imagem e à livre circulação, importa considerar a legitimidade das medidas de polícia eventualmente necessárias para garantir os direitos dos cidadãos, a segurança das pessoas e a manutenção da ordem.

É que, para a prossecução dessas finalidades, a intervenção das forças de segurança deve também respeitar os enunciados critérios de adequação, necessidade e proporcionalidade, tema que se retomará adiante

das situações vitais que, por lhe dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão. O objeto é o bem protegido, que pode ser uma rés (uma coisa, não necessariamente física, no caso de direitos reais) ou um interesse (no caso dos direitos pessoais). No direito à privacidade, o objeto é, sinteticamente, a integridade moral do sujeito. Tanto conteúdo quanto objeto são muito claros no art. 12 da Declaração Universal dos Direitos do Homem de 1948, em que se lê: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicilio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda pessoa tem direito à proteção da lei". No Brasil, a lei n. 5.250/67, ainda em vigor (lei de Imprensa) estabelece responsabilidade civil nos casos de calúnia e difamação e o fato imputado, ainda que verdadeiro, disser "respeito à vida privada do ofendido e a divulgação não foi motivada em razão de interesse público, e a lei n. 7.232/84 — Lei de Informática — protege o sigilo dos dados armazenados, processados e vinculados, que sejam do interesse da privacidade das pessoas (art. 2°, VIII). ”

Hodiernamente, com o incremento dos processos tecnológicos, surgiram vários instrumentos de escuta, internet, fotografias por satélite, o próprio smartphone e instituições que armazenam dados privados, como o Cadin, Serasa, o Serviço de Proteção ao Crédito – SPC, etc., o que potencializa os mecanismos de devassa na vida do cidadão. A multiplicação dos casos de quebra do direito de privacidade fez com que a Constituição brasileira de 1988 adotasse uma proteção a esses direitos.
Intimidade é a esfera de vida que só ao cidadão em particular diz respeito, não pertencendo a mais ninguém; é o espaço de sua individualidade.

O princípio da exclusividade a protege. Vida privada significa as relações pertinentes ao cidadão e aos seus familiares, englobando as pessoas que partilham do seu cotidiano.

5. Do Direito ao Silêncio como Garantia à Não Autoincriminação

5.1- Breve histórico

Sem adentrar tão profundamente, mas buscando supedâneo na brilhante obra de Maria Elizabeth Queijo temos que o *nemo tenetur se detegere* está inserto entre as regras gerais de direito, não sendo possível identificar suas raízes.

Foi no período do Iluminismo que o princípio se firmou. Verifica-se que, historicamente, o princípio *nemo tenetur se detegere* apresenta-se associado ao interrogatório do acusado. Nessa época, marcada pela construção e reconhecimento das garantias penais e processuais penais, que nos dias de hoje parecem tão sedimentadas, tal princípio revela-se como garantia relativa ao resguardo do acusado no interrogatório. Isso decorre do fato de o acusado, nesse período, já não ser visto exclusivamente como objeto da prova.[18]

Posteriormente, o *nemo tenetur* teve forte evolução no direito anglo saxão, sobretudo com a adoção do princípio da dúvida razoável da prova (insuficiência probatória), da presunção de inocência e o desenvolvimento das regras de exclusão de provas.

Mas, foi no início do século XX, e, sobretudo a partir de sua metade, que ganhou os contornos que hoje se apresentam, marcantemente no que diz respeito ao direito a permanecer em silêncio.

Consagrado pela Norma Constitucional e infraconstitucional, todo cidadão tem a garantia de não se autoincriminar. Ela concorre para o direito ao silêncio, a não praticar qualquer ato que possa incriminá-lo e o de não produzir prova contra si (*nemo tenetur re ipsum prodere*).

Oriundo do princípio *nemo tenetur se detegere*, é garantia, e não direito fundamental, posto que aquela, assegura a fruição deste. Na análise de Marcelo Schirmer

[18] QUEIJO, Maria Elizabeth. O direito de não produzir prova contra si mesmo – O princípio do “nemo tenetur se detegere” e suas decorrência no processo penal. 2ª ed. Editora Saraiva. 2012, pp. 31/32

Albuquerque[19] “não há um direito (propriamente dito) ao silêncio, mas, apenas e tão-somente, uma garantia de não autoincriminação, cujo meio de exercício frequentemente é o silêncio”.

Renato Brasileiro de Lima, Promotor de Justiça Militar da União da República Federativa do Brasil, complementa, afirmando que de acordo com o art. 5º, LXIII, da constituição Federal “o preso será informado de seus direitos, entre os quais o de permanecer calado, sendo-lhe assegurada a assistência da família e do advogado”. Acerca do direito ao silêncio, o alusivo autor, com a mestria que lhe é peculiar, complementa “O Direito ao silêncio, previsto na Cartas Magna como direito de permanecer calado, apresenta-se apenas como uma das várias decorrências do *nemo tenetur se detegere*, segundo do qual ninguém é obrigado a produzir provas contra si mesmo. Além da Constituição Federal, o princípio *nemo tenetur se detegere* também se encontra previsto no Pacto Internacional dos Direitos Civis e Políticos (art. 14,3, “g”) e na Convenção Americana Sobre Direitos Humanos, a qual passo a discorrer abaixo.

Ainda sobre o tema, agora em relação a postura do eventual investigado/acusado ante uma investigação ou acusação em sede de ação penal, o referido autor pontua que o *nemo tenetur se detegere* “trata-se de uma modalidade de autodefesa passiva, que é exercida por meio da inatividade do indivíduo sobre quem recai ou pode recair uma imputação. Consiste, grosso modo, na proibição de qualquer medida de coerção ou intimidação do investigado e/ou acusado em processo de caráter sancionatório para a obtenção de uma confissão ou para que colabore em atos que possam ocasionar sua condenação”.

Nesse caso, os desdobramentos do direito de não produzir prova contra si mesmo estão consubstanciados em algumas vertentes, entre as quais, destaco as 05 (cinco) mais importantes, **a)** direito ao silêncio ou direito de ficar calado; **b)** direito de não ser constrangido a confessar a prática de ilícito penal; **c)** inexigibilidade de dizer a verdade;

---

[19] ALBUQUERQUE, Marcelo Schirmer. *A garantia de não auto-incriminação extensão e limites.* Belo Horizonte: Del Rey, 2008.

d) direito de não praticar qualquer comportamento ativo que possa incriminá-lo (tal vertente se desdobra, no direito que o investigado/acusado tem em não fornecer padrões vocais necessários a subsidiar elementos de prova objetivando perícia de voz; o investigado/acusado não é obrigado a fornecer material fluído de seu punho para a realização de perícia grafotécnica e, por fim, o impedimento de prisão, de qualquer espécie, em razão do investigado/acusado se negar a fornecer quaisquer desses materiais e se recusar a participar de reconstituição de crimes) e, ainda, o **e)** direito de não produzir nenhuma prova incriminadora invasiva (intervenções corporais que exigem penetração no organismo humano, tais como exames de sangue, ginecológico, endoscopia, identificação por meio de dentes – arcada dentária e outros), como será detalhado mais à frente.

A Convenção Americana sobre Direitos Humanos, mais conhecida como Pacto de Costa Rica, aprovada em 22 de novembro de 1969 (artigo 8º 2, al. G. " Toda pessoa acusada de delito tem direito a que se presuma sua inocência enquanto não se comprove legalmente sua culpa. Durante o processo, toda pessoa tem direito, em plena igualdade, às seguintes garantias[...]direito de não depor contra si mesma, nem a declarar-se culpada)" O princípio foi reconhecido como garantia mínima aos imputados.[20]

A etimologia da palavra silêncio é dupla, deriva tanto do termo latino *silentium,* significando a abstenção do ato de falar, o estado de uma pessoa que se cala, quanto de outro termo latino *sileo, es, ere, ni,* exprimindo a situação daquele que não revela seu pensamento.[21]

O arguido, querendo, pode dar declarações sobre sua conduta em qualquer oportunidade, seja no inquérito ou qualquer fase processual do *jus persequendi*, essa liberdade de declaração, positivamente, é uma expressão de seu direito de defesa, permitindo-lhe apresentar sua versão dos fatos e, consequentemente, influir diretamente no resultado do processo.

---

[20] Ristori, Adriana Dias Paes, Sobre o o Silêncio do Arguido no interrogatório no Processo Penal Português, ED. Almedina, 2008

[21] idem

No entanto, é-lhe assegurado o direito de não se manifestar, também um exercício de autodefesa, garantido pelo princípio supra referido. Situação esta que não pode ser utilizada em seu desfavor. Tal conduta é vista como uma dimensão negativa, contendo em si a proibição de se compelir o acusado a confessar a prática de um delito ou revelá-lo a autoridade responsável pela apuração do mesmo.

Segundo a maioria dos doutrinadores, essa proteção de silenciar-se é a característica mais flagrante do direito a não autoincriminação.

Além de decorrência do nemo tenetur se detegere, o direito ao silêncio configura manifestação do direito à intimidade que, igualmente, é direito fundamental. Insere-se também entre as liberdades públicas, oponíveis ao Estado. Em seu íntimo, o indivíduo tem o direito de calar, de não se pronunciar a respeito da imputação, de reservar-se em seu interior. A respeito, o Abade Dinouart já afirmava que "O homem nunca é tão dono de si mesmo quanto no silêncio: fora dele, parece derramar-se, por assim dizer, para fora de si e dissipar-se pelo discurso; de modo que ele pertence menos a si mesmo do que aos outros". Em que pese a difusão do direito ao silêncio, com maior ou menor extensão nas diversas legislações, registra-se uma forte tendência à associação do referido direito à culpabilidade do acusado, que vem de longa data, mas que persiste no dia a dia dos Tribunais, nos julgados de primeiro grau, em alguns escritos doutrinários. Aliás, o receio de que o silêncio seja interpretado como manifestação de culpabilidade é determinante para que o acusado não exerça o direito ao silêncio. Tal vinculação decorre de enraizada ideia preconcebida, que remonta ao modelo de processo inglês denominado accused speaks, de que quem é inocente responde às indagações formuladas, porque nada tem a ocultar. Mais do que isso: o inocente brada, grita, manifesta-se, proclamando a sua condição. Ilustrativo, a respeito, o dito popular, por vezes recordado em julgados, de que "quem cala, consente".[22]/[23]

---

[22] Queijo, Maria Elizabeth O direito de não produzir prova contra si mesmo : o princípio nemo tenetur se detegere e suas decorrências no processo penal / Maria Elizabeth Queijo. – 2. ed. – São Paulo : Saraiva, 2012.

No entendimento da autora retro referida, o direito ao silêncio não se aplica nos quesitos referentes a identidade do acusado.

---

[23] Idem. A dignidade é da essência da natureza humana. É considerada um "conceito a priori" preexistente[238]. Assinala-se que a dignidade assegura um mínimo de respeito ao homem pelo só fato de ser homem[239]. Por isso, não resulta de criação normativa. A dignidade humana não abrange apenas a liberdade, mas a garantia de condições mínimas de existência. Por isso, na doutrina, afirma-se que o princípio da dignidade humana reporta-se "às exigências básicas do ser humano no sentido de que ao homem concreto sejam oferecidos os recursos de que dispõe a sociedade para a mantença de uma existência digna, bem como propiciadas as condições indispensáveis para o desenvolvimento de suas potencialidades"[240]. Considera-se, dessa forma, que o aludido princípio abrange a dimensão material e espiritual do ser humano. A dignidade humana passou a integrar o rol dos direitos fundamentais, nas Constituições, em razão de atrocidades cometidas por regimes autoritários[241]. A partir de então tem sido considerada valor supremo e base de todos os outros direitos fundamentais[242]. Com relação ao Poder Público, em razão da tutela da dignidade humana, são inadmissíveis restrições injustificáveis ou desproporcionais dela. Também não são toleradas medidas que importem humilhações, discriminações ou perseguições[243]. Verifica-se, assim, que o nemo tenetur se detegere está intimamente relacionado à proteção da dignidade humana. Desse modo, ainda que não fosse o princípio nemo tenetur se detegere adotado expressamente no direito brasileiro, nem fosse possível extraí-lo dos demais princípios anteriormente mencionados, ainda assim deveria ele ser observado, porque integraria o ordenamento jurídico. É que o nemo tenetur se detegere pode ser considerado imanente ao ordenamento jurídico brasileiro, tendo-se em vista que é representativo de tutela à dignidade humana, expressão máxima dos direitos humanos, agasalhada na Constituição Federal como fundamento da República Federativa do Brasil (art. 1º, III). Em reforço, o art. 5º, § 2º, do texto constitucional, em sua primeira parte, dispõe que os direitos e garantias expressos na Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados. Assim, acolhida a dignidade humana como um dos valores fundamentais do Estado brasileiro, incorpora-se o nemo tenetur se detegere no elenco de direitos fundamentais, como dela decorrente, por força do disposto no aludido art. 5º, § 2º, da Constituição. Em suma, o princípio nemo tenetur se detegere foi acolhido, expressamente, no direito brasileiro com a incorporação ao direito interno do Pacto Internacional dos Direitos Civis e Políticos e da Convenção Americana sobre Direitos Humanos. Por força de tal incorporação, em consonância com o disposto no art. 5º, § 2º, da Constituição Federal, como direito fundamental, a norma que prevê o nemo tenetur se detegere possui hierarquia constitucional, o que foi corroborado pelo art. 5º, § 3º, da Magna Charta, acrescentado pela Emenda Constitucional n. 45, de 2004. Trata-se de um princípio-garantia. Como direito fundamental, não poderá ser suprimido nem mesmo por emenda constitucional. Expressamente também foi previsto no art. 5º, LXIII, da Constituição Federal o direito ao silêncio, uma das decorrências do princípio nemo tenetur se detegere. O princípio em foco decorre igualmente das garantias do devido processo legal e da ampla defesa, mais especificamente na vertente da autodefesa, bem como da presunção de inocência, princípios estes agasalhados na Constituição Federal, em seu art. 5º, LIV, LV e LVII, respectivamente. E, sobretudo, dada a vinculação do princípio nemo tenetur se detegere à preservação da dignidade humana, que é um dos postulados norteadores do Estado brasileiro, como Estado Democrático de Direito (art. 1º, III, da Constituição Federal), possível seria extrair seu reconhecimento no direito brasileiro, mesmo que não fosse expressamente previsto, como direito fundamental decorrente do regime e dos princípios adotados na Constituição. Desse modo, o princípio nemo tenetur se detegere insere-se no ordenamento jurídico brasileiro como direito fundamental, de hierarquia constitucional, ressaltando-se tal aspecto pelas consequências que advirão quanto à interpretação dos dispositivos infraconstitucionais que versam sobre o interrogatório e sobre as provas que dependem da colaboração do acusado para sua produção e pelas limitações que devem ser observadas por eventual nova legislação a esse respeito.

A manifestação dessa garantia é visível no caso de computadores apreendidos no âmbito de duas buscas domiciliares na Inglaterra, sendo que ambos estavam com seus dados encriptados. Seus proprietários foram notificados a entregarem suas senhas na forma do artigo 49 *da Regulation of Investigation Powers Act (RIPA)*.

A questão que se discutiu na decisão inglesa é que tendo sido apreendidos mediante autorização judicial seria legítima a revelação coercitiva da senha face à garantia da Não Autoincriminação? Em resposta a esta pergunta o Tribunal decidiu que:

1) Reconheceu a existência do privilégio contra a autoincriminação na *Commom Law* e no Direito Penal Internacional interligando-o com o Princípio da Presunção de Inocência (artigo 6º da Convenção Europeia de Direitos Humanos. No entanto, entendeu que a lei derroga ou limita esse princípio em certos casos, situação em que o arguido teria que responder a certas questões ou entregar documentos, concluindo, daí, que o princípio não é absoluto;

2) O Tribunal *a quo* entendeu que a revelação da senha, por si só, não seria autoincriminatória e, portanto, não se aplicaria o privilégio interpretando que a senha e os dados encriptados tem uma existência separada e independente da mente dos arguidos, mesmo que admitindo que somente eles tinham conhecimento dos mesmos. Afirmou ainda o Tribunal, que a senha não é incriminatória e sim os dados criptografados. O Tribunal *ad quem* concordou com esta fundamentação, discordando, no entanto, em relação a senha e seu conhecimento, posto que sendo os dados encriptados incriminatórios, e o seu acesso só se dando através da senha, então o conhecimento pode ser incriminatório e, desta forma, seria possível a aplicação do privilégio;

3) Assim, o Tribunal entendeu pela proporcionalidade afirmando que, se os dados estão na posse da polícia ou do MP de forma legal, apenas não estando acessíveis, com a revelação da *password* possibilita-se o seu conhecimento e, sendo legítimo o objetivo conclui-se pela proporcionalidade da medida. Pode-se

> discutir no Direito Português, a colaboração do arguido, podendo ser ativa ou passiva. No primeiro caso, o arguido colaboraria de forma direta (ação), no segundo, de forma indireta (sujeição)[24].

Há que se ressaltar que em *Schmerber v. Cal.* (1966), o Tribunal confirmou a admissão de prova colhida em um exame de sangue por um médico no sentido de permitir a polícia atestar a embriaguez de um arguido mesmo com sua objeção. O Tribunal, por uma decisão de 5 x 4 rejeitou a alegação de que a admissão da amostra violou a quinta emenda no que diz respeito ao arguido não ser obrigado, em qualquer processo penal, ser uma testemunha contra si próprio." A fundamentação da maioria é que "o privilégio protege um arguido apenas de ser obrigado a depor contra si próprio ou fornecer, de outra forma ao Estado a evidência de um depoimento de natureza comunicativa." Como o Tribunal decidiu mais tarde, o privilégio protege a manifestação do "conteúdo da sua mente."[25]

O Direito de não autoincriminação contém várias dimensões (direito ao silêncio, direito de não declarar com si próprio, direito de não confessar, direito de não ceder seu corpo para produção de prova etc.). Dentre elas está, evidentemente, o direito ao silêncio, que está contemplado expressamente tanto na Constituição da República Federativa do Brasil como na Convenção Americana sobre Direitos Humanos, embora outras legislações, inclusive a portuguesa, permita o uso das chamadas provas invasivas, como, v.g., a colheita de sangue para exame de DNA no arguido.

O próprio Código de Processo Penal Português, proíbe, no seu artigo 126, n.º. que a prova obtida mediante intromissão na vida privada sem o consentimento do titular do direito está a determinar a necessidade das autoridades públicas, designadamente

---

[24] Pinto, Sofia Lara. Coord. Tereza Pizarro Beleza e Frederico de Lacerda da Costa Pinto. *Prova Criminal e Direito de defesa: Estudos sobre Teoria de prova e garantias de defesa em processo penal.* Ed. Almedina S.A. 2ª reimpressão.2013

[25] LaFave, Wayne R. Israel, Jerold H.King, Nancy J. Kerr, Orin S. *Criminal Procedure.* Série HORNBOOK®. Ed. 2015 (tradução livre)

investigadores e autoridades judiciárias, respeitarem os direitos fundamentais dos cidadãos quando da perseguição criminal.[26]

5.2 - Do *nemo tenetur se ispum accusare*

O direito de permanecer calado corresponde ao núcleo duro da garantia contra a autoincriminação, estando consagrado em todos os ordenamentos jurídicos democráticos.

Possui a estrutura normativa de regra identificando-se com o conteúdo essencial absoluto do *nemo tenetur,* e não pode ser restringido[27]

É fato que um dos principais fatores de distinção entre os sistemas processuais inquisitivo e acusatório consiste que, no inquisitivo, a confissão deve ser extorquida da boca do réu, enquanto que, no segundo, o acusado não pode ser compelido a produzir manifestações de cunho intelectual ou testemunhal, que é exatamente o que se protege no caso *sub examen.* Revelando a senha, o arguido estaria depondo em seu desfavor, o que gerou a proteção judicial.

É importante frisar que o silêncio do acusado não poderá ser interpretado em seu desfavor, posto que inconcebível o exercício de um direito resultar em prejuízo processual para o acusado.

O direito ao silêncio é só uma parte do direito de não autoincriminação: não se pode nunca confundir a parte com o todo. O direito ao silêncio (direito de ficar calado), previsto constitucionalmente (art. 5º, inc. LXIII, da CF), constitui somente uma parte do direito de não autoincriminação. Como emanações naturais diretas desse direito (ao

---

[26] Martins, Milene Viegas . A Admissibilidade de Valoração de Imagens captadas por particulares comp prova no processo penal penal, Ed. Associação Acadêmica da Faculdade de Direito de Lisboa. 1ª ed. 2014.

[27] Filho, Wagner Marteleto. *O* direito a não autoincrminação no processo penal contemporâneo.Editora Del Rey, 1ª ed. 2012.

silêncio) temos: (a) o direito de não colaborar com a investigação ou a instrução criminal; (b) o direito de não declarar contra si mesmo; (c) o direito de não confessar e (d) o direito de não falar a verdade.[28]

Essas cinco dimensões acham-se coligadas diretamente ao silêncio, que afeta a produção da prova. Disso decorre a evidente conclusão de que o direito ao silêncio implica uma relevante questão probatória; constitui, aliás, um dos limites ao princípio da liberdade de provas. Todas as demais dimensões do direito à não autoincriminação reconhecidas pela jurisprudência tem essa mesma origem limitativa ao direito à prova.

O direito ao silêncio (previsto expressamente na CF brasileira) exprime, acima de tudo, que do acusado não se pode exigir que contribua ou que produza ou que participe ativamente de qualquer procedimento probatório que o incrimine.

Nesse mesmo diapasão está o direito de não declarar contra si mesmo assim como o direito de não confessar (ambos previstos na CADH art. 8º, 2, g e no PIDCP art. 14, 3, g). A leitura desses textos normativos poderia nos conduzir a uma interpretação restritiva do direito fundamental à não autoincriminação, para concluir que ele valeria apenas (e exclusivamente) em relação aos atos" comunicacionais "(declarações, confissões etc.). Na verdade, não importa se o meio probatório é oral ou documental (escrito) ou material ou corporal ou puramente procedimental.

O direito de ficar calado, previsto na Constituição brasileira (CF, art. 5º, inc. LXIII), assim como o direito de não declarar ou o direito de não confessar (previstos nos tratados internacionais), não podem ser interpretados restritivamente. Por força do princípio da máxima efetividade dos direitos fundamentais (que são vinculantes e de aplicação direta e imediata CF, art. 5º, 1º), onde existe a mesma razão (*ratio legis*), deve preponderar o mesmo direito. Se a razão de conferir ao réu o direito ao silêncio está no seu direito de não se auto incriminar, onde este último direito der o ar da sua

[28] LIMA, Aldo Corrêa de. *PRINCÍPIO DA NÃO AUTO-INCRIMINAÇÃO (DIREITO AO SILÊNCIO, POR EXEMPLO*). https://aldoadv.wordpress.com/2010/01/26/principio-da-nao-auto-incriminacao-significadoconteudo-base-juridica-e-ambito-de-incidencia/ [9] Ibidem.

presença (da sua graça), o mesmo direito, ou seja, as mesmas consequências do direito ao silêncio hão de vingar. É nesse raciocínio (lógico e dedutivo) que descansa a base constitucional e internacional não só do direito ao silêncio, senão também de todas as (nove) dimensões da não autoincriminação. Para não se incriminar o réu tem até o direito de mentir, porém, também esse direito tem limite: não pode prejudicar terceiros.[29]

No caso *sub examen,* o Juiz ressaltou que a senha só existia na mente do suspeito e assim, obriga-lo a fornecê-la constituiria um depoimento contra si próprio, em clara ofensa a 5ª emenda. Entendeu ainda que, a proteção do *smartphone* via biometria não se enquadra sob a proteção da referida emenda pois não exigia a transmissão de conhecimento.[30]

No mesmo sentido em *Riley v. California*[31], em passado recente, a Suprema Corte Americana decidiu, revertendo uma decisão unânime de primeira instância, que, em geral, a polícia não pode procurar informações contidas em um *smartphone* apreendido com um cidadão que foi preso, salvo se houvesse mandado judicial.

No entanto, no mesmo caso, a Suprema Corte deixou claro que, em muitos aspectos o aparelho "é uma extensão da pessoa, pois traz em si, informações íntimas do ser, elaborações mentais que só são feitas quando se presume que terceiros não terão acesso.[32]

Fato semelhante se deu na Pensilvânia quando um Juiz Federal determinou que os réus em um caso de informações privilegiadas não podem ser obrigados a divulgar suas senhas de smartphones para a Comissão de Valores Mobiliários (cujo acrônimo é

---

[29] GOMES, Luiz Flávio. Princípio da não autoincriminação: significado, conteúdo, base jurídica e âmbito de incidência. Disponível em http://www.lfg.com.br 26 janeiro. 2010.
[30] Harvard Journal of Law and Technology.

[31] ESTADOS UNIDOS DA AMÉRICA. Suprema Corte dos Estados Unidos. Decisão Riley v. California, California, 25 de Junho de 2014.
[32] http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

SEC em Inglês). O Juiz Mark Kearney escreveu, “Como a SEC não está à procura de registros de negócios, mas dos processos de pensamento pessoais dos Réus”, eles têm o direito de invocar a Quinta Emenda e garantir seu direito a proteção contra a autoincriminação.[33]

Na *American Criminal Review* temos que os Juízes reconheceram que chamar um *smartphone* de telemóvel é um termo impróprio, posto que os mesmos contêm muito mais dados que um simples aparelho de comunicação móvel.
As circunstâncias de acesso a estes aparelhos trazem implicações que ferem os direitos individuais de privacidade. No caso da vedação de autoincriminação, o reconhecimento de que se tratava de uma garantia fundamental para todo cidadão estadunidense foi consagrado com o julgamento do caso *Miranda v. Arizona, 384 U.S. 436 (1966)14.*[34]

A decisão da Suprema Corte foi tomada por apertada maioria de 5 votos *(Earl Warren, Hugo Black, William Douglas, William Brennan e Abe Fortas*) a 4 (*John Marshall Harlan, Potter Stewart, Byron White e Tom Clark*). Nessa decisão, a Suprema Corte estabeleceu que devido à natureza coercitiva inerente a um interrogatório policial, nenhuma confissão seria admissível em razão da garantia de não se auto incriminar, a menos que o suspeito fosse previamente cientificado de seu direito de ser assistido por um advogado.
Julgado no mesmo ano que *Miranda v. Arizona,* o caso *Schmerber v. California*[35], 384 U.S.757 (1966) é importante para fixar os contornos da garantia de vedação de autoincriminação nos EUA.

Em nova decisão tomada, também, por apertada maioria de 5 votos (*William Brennan, John Marshall Harlan, Potter Stewart, Byron White e Tom Clark*) a 4 (*Earl Warren, Hugo*

---

[33] http://www.brc.com.br/juiz-federal-diz-que-reus-nao-podem-ser-forcados-a-revelar-senhas/

[34] ESTADOS UNIDOS DA AMÉRICA. Suprema Corte dos Estados Unidos. Decisão Miranda v. Arizona, Arizona, 13 de Junho de 1966.

[35] ESTADOS UNIDOS DA AMÉRICA. Suprema Corte dos Estados Unidos. Schmerber v. California, 1966.

Black, William Douglas, Abe Fortas), a Suprema Corte rejeitou a alegação de que o sangue retirado do indivíduo sem autorização violava a garantia de não auto incriminar, reafirmando o entendimento de que a garantia compreende exclusivamente o direito de não ser compelido ou coagido a fornecer declarações ou depoimentos, ou qualquer outra manifestação de natureza comunicativa, seja oral ou escrita que possa incriminá-lo.

Responsável pela definição do julgamento 15 e relator da decisão, o Juiz William Brennan, fixou as seguintes diretrizes para essa nova situação:

a) O alcance da garantia de não se auto incriminar deve proteger o indivíduo apenas contra medidas que violem seu direito de decidir sobre se quer ou não participar do processo criminal por meio de declarações ou depoimentos;

b) A Suprema Corte não deve modificar o entendimento estabelecido no caso *Holt v. United States, 218 U.S. 245 (1910)* em que considerara admissível a sujeição do indivíduo para que vestisse determinada roupa a fim de participar de ato de reconhecimento para fins criminais;

c) Por conseguinte, a garantia de não se auto incriminar não compreendia uma vedação ao uso do corpo do indivíduo como meio de prova, tais como obtenção de impressões digitais, de fotos, de padrões gráficos ou vocais para exame pericial, bem como a possibilidade de impor o comparecimento do réu em juízo e, ainda, que fizesse um gesto determinado para efeitos de reconhecimento;

d) Da mesma forma, a retirada de sangue mediante a perfuração da pele para obtenção de materiais que pertençam ao indivíduo, e cujo exame pericial poderá ser utilizado como prova em processo criminal, não implica em nenhuma espécie de compulsão para prestar depoimentos e que sua participação, exceto como doador, é irrelevante, já que a prova não fora produzida por meio de métodos que violassem sua liberdade de formação da vontade, de depoimento ou de comunicação, mas por uma análise química.[17]

Finalmente é importante afirmar que, em primeira instância o acusado David Charles Baust foi absolvido das acusações a ele imputadas e que as informações contidas no seu smartphone não foram franqueadas a acusação, tornando o caso fraco para o Ministério Público[18] garantindo sua absolvição.

6 - Provas ilícitas por Derivação: A Teoria dos frutos da árvore envenenada e seu nexo de causalidade com o *nemo tenetur*

No magistério de Wagner Marteleto Filho, temos que a proibição de utilização da prova ilícita vai além da exclusão da própria prova produzida com violação de direitos ou garantias fundamentais. O que se discute é o alcance dessa proibição, ou seja, se esta "abarca a prova mediata, e em que medida o faz." Trata-se do efeito à distância (Fernwirkung) do direito alemão ou da *fruit of the poisonous tree doctrine* (Teoria dos frutos da árvore venenosa) do direito americano.)[36]

Em razão dessa teoria, a prova originada daquela obtida por meios ilícitos também é inadmissível, posto que contaminada por aquela. Essa teoria, originou-se do direito Norte americano (1920), no caso *Silverstone Lumber Co. v. U.S., 251 U.S. 385* onde houve uma apreensão ilegal de documentos. Após tal apreensão, os acusados foram intimados a apresentar os mesmos documentos, que lhes foram devolvidos por decisão judicial, sendo que a Corte decidiu pela exclusão dos mesmos pois estariam maculados por investigação inconstitucional.

A regra de exclusão (exclusionary rule) das provas derivadas daquelas obtidas ilicitamente comporta, na jurisprudência da Suprema Corte dos EUA, diversas exceções, tendo sido recepcionadas no ordenamento jurídico brasileiro, no art. 157, §§ 1º e 2º do CPP, ao menos duas delas: a) fonte independente e b) descoberta inevitável.

---

[36] Filho, Wagner Marteleto – O Direito à não autoincriminação no processo penal contemporâneo. P.208, 1ªed. Editora Del Rey, 2012, p.208.

A reforma legislativa de 2008, introduzida pela Lei 11.690, visou a modernização do Código de Processo Penal e a sua conformação à Constituição de 1988, alterando substancialmente a teoria geral da prova penal ao dar nova redação aos arts. 155, 156, 157, 159, 201, 210 e 212 do Código e, particularmente sobre o tema relacionado à prova ilícita, a ele se refere expressamente o art. 157, que passou a ter a seguinte redação: "São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a princípios ou normas constitucionais", inserindo ainda tratamento próprio em relação às provas ilícitas por derivação e à recepção da teoria da fonte independente, embora mesclando esta com a teoria " - da descoberta inevitável. Na dicção do § 2o Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova". Há, ainda, expressa previsão de exclusão da prova ilícita dos autos: §3º. Preclusa a decisão de desentranhamento da prova declarada ilícita, serão tomadas as providências para o arquivamento sigiloso em cartório".[37]

Ainda na lição de Sérgio Ricardo de Souza, "A teoria dos frutos da árvore envenenada (the fruits of the poisonous tree) tem suas origens na Suprema Corte Americana73 e baseia-se na tese bíblica de que, a exemplo do que ocorre com uma árvore doente, que produz frutos também doentes, a prova obtida ilicitamente contamina os seus frutos, ou seja, as demais provas que tenham sido descobertas e produzidas apenas em decorrência das informações obtidas ilicitamente, como ocorre, por exemplo, quando a partir de uma tortura se obtém a informação do local onde se encontra escondido o documento falsificado que servirá de base exclusiva à denúncia, ou ainda, quando a partir de uma busca e apreensão sem autorização judicial se apreende o produto do crime.

Até o advento da Lei 11.690/2008, cujo §I, do art. 157, estabelece que "são também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de

[37] SOUZA, Sérgio Ricardo de, Manual da Prova Penal Constitucional, Editora Juruá, 3ª edição Revista e atualizada, p.39.

causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras", não havia previsão legal expressa de proibição da prova ilícita por derivação, sendo que o acolhimento da tese decorria de uma interpretação sistemática da norma constitucional que veda a utilização da prova ilícita no processo (CRFB, art. 5o, LVI) e do princípio do devido processo legal (CRFB, art. 5o, LIV)."[38]/[39]

Ad argumentadum e, por via analógica, temos que, no caso em exame, o possível uso dos dados contidos no smartphone apreendido em poder de David Baust, mesmo que não houvesse restrições no mandado de busca e apreensão expedido, o que não era o

---

[38] Idem, p.41

[39] STF: A Questão da Doutrina dos Frutos da Arvore Envenenada (Fruits Of The Poisonous Tree): A Questão Da Ilicitude Por Derivação. - Ninguém pode ser investigado, denunciado ou condenado com base, unicamente, em provas ilícitas, quer se trate de ilicitude originária, quer se cuide de ilicitude por derivação. Qualquer novo dado probatório, ainda que produzido, de A modo válido, em momento subsequente, não pode apoiar-se, não pode ter fundamento causal nem derivar de prova comprometida pela mácula da ilicitude originária. - A exclusão da prova originariamente | ilícita - ou daquela afetada pelo vício da ilicitude por derivação - representa um dos meios mais expressivos destinados a conferir efetividade à garantia do "due process of law" e a tomar mais intensa, pelo | banimento da prova ilicitamente obtida, a tutela constitucional que | preserva os direitos e prerrogativas que assistem a qualquer acusado J em sede processual penal. Doutrina. Precedentes. A doutrina da ilicitude por derivação (teoria dos "frutos da árvore envenenada") repudia, por constitucionalmente inadmissíveis, os meios probatórios, que, J não obstante produzidos, validamente, em momento ulterior, acham- \ se afetados, no entanto, pelo vicio (gravíssimo) da ilicitude originária, \ que a eles se transmite, contaminando-os, por efeito de repercussão 3 causai. Hipótese em que os novos dados probatórios somente foram j conhecidos, pelo Poder Público, em razão de anterior transgressão | praticada, originariamente, pelos agentes da persecução penal, que j desrespeitaram a garantia constitucional da inviolabilidade domiciliar. \

- Revelam-se inadmissíveis, desse modo, em decorrência da ilicitude | por derivação, os elementos probatórios a que os órgãos da persecução penal somente tiveram acesso em razão da prova originariamente j ilícita, obtida como resultado da transgressão, por agentes estatais, 1 de direitos e garantias constitucionais e legais, cuja eficácia condicionante, no plano do ordenamento positivo brasileiro, traduz significativa limitação de ordem jurídica ao poder do Estado em face dos cidadãos. - Se, no entanto, o órgão da persecução penal demonstrar 1 que obteve, legitimamente, novos elementos de informação a partir de < uma fonte autônoma de prova - que não guarde qualquer relação de dependência nem decorra da prova originariamente ilícita, com esta não mantendo vinculação causai —, tais dados probatórios revelar-se-ão plenamente admissíveis, porque não contaminados pela mácula da ilicitude originária. - A questão da fonte autônoma de prova ("an independent source ") e a sua desvinculação causal da prova ilicitamente obtida - Doutrina - Precedentes do Supremo Tribunal Federal

- Jurisprudência Comparada (A Experiência Da Suprema Corte Americana): Casos "Silverthorne Lumber Co. V. United States (1920); Segura V. United States (1984); Nix V Williams (1984); Murray V. United States (1988) ". (STF - RHC 90376 / RJ - Rei. Min. Celso de Mello - Publ. DJ 18.05.2007 - p. 113). STF: Sentença condenatória fundada em provas ilícitas. Inocorrência da aplicação da teoria dos "frutos da árvore envenenada" Provas autônomas. Desnecessidade de desentranhamento da prova ilícita. Impossibilidade de aplicação do art. 580 do CPP à espécie. Inocorrência de ofensa aos arts. 59 e 68 do Código Penal. Habeas corpus indeferido. Liminar cassada. 1. A prova tida como ilícita não contaminou os demais elementos do acervo probatório, que são autônomos, não havendo motivo para a anulação da sentença. 2. Desnecessário o desentranhamento dos autos da prova declarada ilícita, diante da ausência de qualquer resultado prático em tal providência, considerado, ademais que a ação penal transitou em julgado (HC 89032 / SP - STF - Rei. Min. Menezes Direito - Publ. DJ 23.11.2007 - p. 79).

caso, a prova seria inadmissível, face ao seu vínculo de origem com a prova que seria ilícita por ferir o *nemo tenetur*.

Existem provas em Processo Penal que, em razão do princípio da verdade real, o acusado acaba submetido, quer pelo Juiz, Ministério Público ou autoridade policial, a intervenção em seu corpo para que as mesmas sejam produzidas. Por essa razão, o princípio *nemo tenetur se detegere* serve como barreira à atividade investigatória e probatória ilimitada por parte do Estado.

7 - Do Direito ao Silêncio

O direito de ficar calado, previsto na Constituição brasileira (CF, art. 5º, inc. LXIII), assim como o direito de não declarar ou o direito de não confessar (previstos nos tratados internacionais), não podem ser vistos de forma restritiva. Por força do princípio da máxima efetividade dos direitos fundamentais (que são vinculantes e de aplicação direta e imediata CF, art. 5º, 1º), onde existe a mesma razão (*ratio legis*), deve preponderar o mesmo direito. Se a razão de conferir ao réu o direito ao silêncio está no seu direito de não se autoincriminar, onde este último direito estiver presente, o mesmo direito, ou seja, as mesmas consequências do direito ao silêncio hão de vingar. É nesse raciocínio (lógico e dedutivo) que descansa a base constitucional e internacional não só do direito ao silêncio, senão também de todas as (nove) dimensões da não autoincriminação. Para não se incriminar o réu tem até o direito de mentir, porém, também esse direito tem limite: não pode prejudicar terceiros.

O sistema norte-americano vem sendo citado como exemplo dessa interpretação restritiva do direito de não autoincriminação, sobretudo a partir da decisão da Suprema Corte, proferida no Caso Schmerber vs. Califórnia, em 1966. Por 5 votos a 4 a Corte

delimitou o direito de não autoincriminação às declarações comunicativas do réu, orais ou escritas, conforme citado anteriormente.[40]

Cuida-se de restrição que no sistema brasileiro seria inconstitucional e inconvencional, porque do direito ao silêncio, do direito de não declarar contra si mesmo e do direito de não confessar (CF, art. 5º, LXIII; CADH, art. 8º, 2, g; PIDCP, art. 14.3, g) fazem parte, implícita e naturalmente, todas as demais dimensões da não autoincriminação, que tem seu núcleo essencial fundado em uma inatividade (ou em uma atividade não prejudicial a terceiros). Nesse sentido é a consolidada jurisprudência do STF, sendo disso exemplo o HC 96.219, rel. Min. Celso de Mello, que sublinhou

"A recusa em responder ao interrogatório policial e/ou judicial e a falta de cooperação do indiciado ou do réu com as autoridades que o investigam ou que o processam traduzem comportamentos que são inteiramente legitimados pelo princípio constitucional que protege qualquer pessoa contra a autoincriminação, especialmente aquela exposta a atos de persecução penal. "O Estado - que não tem o direito de tratar suspeitos, indiciados ou réus como se culpados fossem (RTJ 176/805-806) - também não pode constrangê-los a produzir provas contra si próprios (RTJ 141/512)."Aquele que sofre persecução penal instaurada pelo Estado tem, dentre outras prerrogativas básicas, o direito (a) de permanecer em silêncio, (b) de não ser compelido a produzir elementos de incriminação contra si próprio nem constrangido a apresentar provas que lhe comprometam a defesa e (c) de se recusar a participar, ativa ou passivamente, de procedimentos probatórios que lhe possam afetar a esfera jurídica, tais como a reprodução simulada do evento delituoso e o fornecimento de padrões gráficos ou de padrões vocais, para efeito de perícia criminal. Precedentes." O exercício do direito contra a autoincriminação, além de inteiramente oponível a qualquer autoridade ou agente do Estado, não legitima, por efeito de sua natureza constitucional, a adoção de medidas que afetem ou restrinjam a esfera jurídica daquele contra quem se instaurou a "*persecutio criminis*."

---

[40] GOMES, Luiz Flávio*. Princípio da não autoincriminação: significado, conteúdo, base jurídica e âmbito de incidência.* Disponível em http://www.lfg.com.br 26 janeiro. 201

Já em Portugal, o acusado não pode recusar-se a submeter-se à perícia, podendo ser obrigado a fazê-lo. O Tribunal Constitucional, amparado por posição firmada pelo Tribunal Europeu de Direitos Humanos no caso *Saunders v. United Kingdom* admite apenas a não autoincriminação através das declarações do arguido (direito de permanecer em silêncio).[41]

Recente decisão do Superior Tribunal de Justiça, embora não se aborde o assunto de quebra de criptografia, mas na mera obtenção de dados do smartphone sem autorização judicial decidiu que "a análise dos dados telefônicos constante dos aparelhos dos investigados, sem sua prévia autorização ou de prévia autorização judicial devidamente motivada, revela a ilicitude da prova.

Sem prévia autorização judicial, são nulas as provas obtidas pela polícia por meio da extração de dados e de conversas registradas no whatsapp presentes no celular do suposto autor de fato delituoso, ainda que o aparelho tenha sido apreendido no momento da prisão em flagrante**.** STJ. 6ª Turma. RHC 51.531-RO, Rel. Min. Nefi Cordeiro, julgado em 19/4/2016 (Info 583).[42]

---

[41] Op.cit

[42] TJ-CE - Habeas Corpus HC 06261942420158060000 CE 0626194-24.2015.8.06.0000 (TJ-CE) Data de publicação: 22/09/2015

Ementa: PENAL E PROCESSO PENAL. HABEAS CORPUS. TENTATIVA DE HOMICÍDIO. NULIDADE DE

PROVAS ILÍCITAS. QUEBRA DE SIGILO TELEFÔNICO. INOCORRÊNCIA. A ANÁLISE DAS MENSAGENS TELEFÔNICAS DO CELULAR DO RÉU SE DERAM EM DECORRÊNCIA DA PRISÃO DO PACIENTE. AUSÊNCIAPrecisa de uma DE PERÍCIA TÉCNICA. PRESCINDÍVEL. PRELIMINAR REJEITADA. 1. O paciente foi preso por força, decisão da f deorientação jurídica? mandado de prisão temporária desde 21.05.2015, pela suposta prática do crime de tentativa de homicídio, contra a vítima Gleuson de Almeida Leite. 2. Em sede de preliminar, aduz a nulidade da prova que embasou a decretação de sua segregação cautelar, posto que ilícita, já que trata-se de mensagens de texto do aplicativo whatsapp retirada de seu celular, sem autorização judicial, bem como desacompanhada de laudo pericial, para atestar de qual celular originou tais mensagens. 3 . A Jurisprudência Pátria vem entendendo que a garantia1 constitucional da inviolabilidade das comunicações telefônicas se refere, especificamente, à vedação de escutas clandestinas, a qual não se coaduna a verificação das mensagens de texto ou das últimas ligações recebidas ou efetuadas de celulares apreendidos na posse de suspeitos da prática de crimes, sendo certo que o artigo 6º , incisos II e III , do Código de Processo Penal determina ser dever da Autoridade Policial apreender os objetos que tiverem relação com o fato, o que, no presente caso, significa saber se os dados constantes nos aplicativos de mensagem dos aparelhos celulares apreendidos trariam alguma prova do envolvimento do agente com a tentativa de homicídio. PRECEDENTES. 4. Outrossim, também inexiste qualquer nulidade em razão da não realização de perícia nas mensagens anexadas aos autos da ação penal. A legislação e jurisprudência pátria, não exigem como elemento de validade de transcrição de mensagem de texto extraídas de

No Brasil, temos, em sentido contrário, decisão do Superior Tribunal de Justiça, na famosa Operação Lava-jato.[43]

(RHC 75.800/PR, Rel. Ministro FELIX FISCHER, QUINTA TURMA, julgado em 15/09/2016, DJe 26/09/2016)[44]/[45]

---

celular, que a mesma esteja devidamente acompanhada de laudo pericial, especialmente no caso da decretação da prisão preventiva, onde exige-se apenas indícios simples...

[43] Ementa Ofcial
PROCESSUAL PENAL. OPERAÇÃO "LAVA-JATO". MANDADO DE BUSCA E APREENSÃO. APREENSÃO DE APARELHOS DE TELEFONE CELULAR. LEI 9296/96.
OFENSA AO ART. 5º, XII, DA CONSTITUIÇÃO FEDERAL. INOCORRÊNCIA.
DECISÃO FUNDAMENTADA QUE NÃO SE SUBORDINA AOS DITAMES DA LEI 9296/96. ACESSO AO CONTEÚDO DE MENSAGENS ARQUIVADAS NO APARELHO.
POSSIBILIDADE. LICITUDE DA PROVA. RECURSO DESPROVIDO.
I - A obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei 9296/96.
II - O acesso ao conteúdo armazenado em telefone celular ou smartphone, quando determinada judicialmente a busca e apreensão destes aparelhos, não ofende o art. 5º, inciso XII, da Constituição da República, porquanto o sigilo a que se refere o aludido preceito constitucional é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados, e não dos dados em si mesmos.
III - Não há nulidade quando a decisão que determina a busca e apreensão está su cientemente fundamentada, como ocorre na espécie.
IV - Na pressuposição da ordem de apreensão de aparelho celular ou smartphone está o acesso aos dados que neles estejam armazenados, sob pena de a busca e apreensão resultar em medida írrita, dado que o aparelho desprovido de conteúdo simplesmente não ostenta virtualidade de ser utilizado como prova criminal.
V - Hipótese em que, demais disso, a decisão judicial expressamente determinou o acesso aos dados armazenados nos aparelhos eventualmente apreendidos, robustecendo o alvitre quanto à licitude da prova.
Recurso desprovido.

[44] RHC 75.800/PR, Rel. Ministro FELIX FISCHER, QUINTA TURMA, julgado em 15/09/2016, DJe 26/09/2016)

[45] PENAL. PROCESSUAL PENAL. RECURSO ORDINÁRIO EM HABEAS CORPUS. TRÁFICO DE DROGAS. NULIDADE DA PROVA. AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL PARA A PERÍCIA NO CELULAR. CONSTRANGIMENTO ILEGAL EVIDENCIADO.
1. Ilícita é a devassa de dados, bem como das conversas de whatsapp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial.
2. Recurso ordinário em habeas corpus provido, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos.
(RHC 51.531/RO, Rel. Ministro NERI CORDEIRO, SEXTA TURMA, julgado em 19/04/2016, DJ 09/05/2016) .

No Brasil, a jurisprudência moderna vai em sentido contrário conforme se vê abaixo:
RECURSO EM HABEAS CORPUS Nº 89.981 - MG (2017/0250966-3)
RELATOR : MINISTRO REYNALDO SOARES DA FONSECA
RECORRENTE : JUNIO GUEDES FERREIRA
ADVOGADOS : GUILHERME RIBEIRO GRIMALDI E OUTRO (S) - MG129232 JULIO CESAR BATISTA SILVA - MG085191
RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS
EMENTA
PENAL E PROCESSO PENAL. RECURSO EM HABEAS CORPUS. FURTO E QUADRILHA. APARELHO TELEFÔNICO APREENDIDO. VISTORIA REALIZADA PELA POLÍCIA MILITAR SEM AUTORIZAÇÃO JUDICIAL OU DO PRÓPRIO INVESTIGADO. VERIFICAÇÃO DE MENSAGENS ARQUIVADAS. VIOLAÇÃO DA INTIMIDADE. PROVA ILÍCITA. ART. 157 DO CPP. RECURSO EM HABEAS CORPUS PROVIDO.

1. Embora a situação retratada nos autos não esteja protegida pela Lei
n. 9.296/1996 nem pela Lei n. 12.965/2014, haja vista não se tratar de quebra sigilo telefônico por meio de interceptação telefônica, ou seja, embora não se trate violação da garantia de inviolabilidade das comunicações, prevista no art. 5º, inciso XII, da CF, houve sim violação dos dados armazenados no celular do recorrente (mensagens de texto arquivadas - WhatsApp).
2. No caso, deveria a autoridade policial, após a apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados armazenados, haja vista a garantia, igualmente constitucional, à inviolabilidade da intimidade e da vida privada, prevista no art. 5º, inciso X, da CF. Dessa forma, a análise dos dados telefônicos constante dos aparelhos dos investigados, sem sua prévia autorização ou de prévia autorização judicial devidamente motivada, revela a ilicitude da prova, nos termos do art. 157 do CPP. Precedentes do STJ.
3. Recurso em habeas corpus provido, para reconhecer a ilicitude da colheita de dados do aparelho telefônico dos investigados, sem autorização judicial, devendo mencionadas provas, bem como as derivadas, serem desentranhadas dos autos.

ACÓRDÃO
Vistos, relatados e discutidos os autos em que são partes as acima indicadas, acordam os Ministros da Quinta Turma do Superior Tribunal de Justiça, por unanimidade, dar provimento ao recurso, nos termos do voto do Sr. Ministro Relator. Os Srs. Ministros Ribeiro Dantas, Joel Ilan Paciornik e Jorge Mussi votaram com o Sr. Ministro Relator.
Ausente, justificadamente, o Sr. Ministro Felix Fischer.
Brasília (DF), 05 de dezembro de 2017(Data do Julgamento)
Ministro REYNALDO SOARES DA FONSECA
RECURSO EM HABEAS CORPUS Nº 89.981 - MG (2017/0250966-3) RELATOR : MINISTRO REYNALDO SOARES DA FONSECA RECORRENTE : JUNIO GUEDES FERREIRA
ADVOGADOS : GUILHERME RIBEIRO GRIMALDI E OUTRO (S) - MG129232 JULIO CESAR BATISTA SILVA - MG085191
RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS

RELATÓRIO

O EXMO. SR. MINISTRO REYNALDO SOARES DA FONSECA:
Trata-se de recurso ordinário em habeas corpus, com pedido de liminar, interposto por JUNIO GUEDES FERREIRA, contra acórdão do Tribunal de Justiça do Estado de Minas Gerais que denegou a ordem no HC n. 1.0000.17.056134-4.
Depreende-se dos autos que o recorrente foi denunciado pela suposta prática dos crimes previstos nos artigos 155, § 4º, IV, c/c o artigo 14, II, e 288, todos do Código Penal.
A defesa impetrou prévio mandamus perante a Corte local objetivando a declaração de nulidade da ação penal, restando a ordem denegada. Eis a ementa do julgado (e-STJ fl. 114):
EMENTA: HABEAS CORPUS - CRIME DE FURTO QUALIFICADO
- ASSOCIAÇÃO CRIMINOSA - NULIDADE POR ILEGALIDADE E ILICITUDE DAS PROVAS PRODUZIDAS - AUSÊNCIA DE CONSTRANGIMENTO ILEGAL EVIDENTE - ORDEM DENEGADA.
- O habeas corpus não se presta ao exame aprofundado de questões meritórias, a não ser que se verifique patente constrangimento ilegal, o que não ocorre in casu.
- Diante da ausência de manifesto constrangimento ilegal, sanável de ofício, denega-se a ordem.
- Ordem denegada.
Daí o presente recurso, no qual a defesa alega ser necessária a declaração de nulidade do procedimento criminal, por terem sido as provas que respaldaram o oferecimento da denúncia consistentes em mensagens constantes de aplicativo de whatsapp obtidas sem autorização judicial e sem a autorização do acusado.

Requer, liminarmente, a suspensão da Ação Penal n.0065383-19.2016.8.13.0456 até final julgamento deste writ. No mérito, pleiteia a declaração de nulidade do procedimento criminal.
Indeferido o pleito liminar e prestadas as informações solicitadas (e-STJ fls. 150/151), opinou o Ministério Público Federal "pelo conhecimento e provimento do recurso ordinário", em parecer assim ementado (e-STJ fl. 161):

PENAL E PROCESSO PENAL. FURTO QUALIFICADO TENTADO E ASSOCIAÇÃO CRIMINOSA. PRISÃO EM FLAGRANTE CONVERTIDA EM PREVENTIVA. RECEBIMENTO DA DENÚNCIA. HABEAS CORPUS IMPETRADO NA CORTE ESTADUAL. ORDEM DENEGADA. RECURSO.
“A JURISPRUDÊNCIA DAS DUAS TURMAS DA TERCEIRA SEÇÃO DESTE TRIBUNAL SUPERIOR FIRMOU - SE NO SENTIDO DE SER ILÍCITA A PROVA OBTIDA DIRETAMENTE DOS DADOS CONSTANTES DE APARELHO CELULAR , DECORRENTES DE MENSAGENS DE TEXTOS SMS, CONVERSAS POR MEIO DE PROGRAMA OU APLICATIVOS ('WHATSAPP'), MENSAGENS ENVIADAS OU RECEBIDAS POR MEIO DE CORREIO ELETRÔNICO, OBTIDOS DIRETAMENTE PELA POLÍCIA NO MOMENTO DO FLAGRANTE, SEM PRÉVIA AUTORIZAÇÃO JUDICIAL PARA ANÁLISE DOS DADOS ARMAZENADOS NO TELEFONE MÓVEL” – PRECEDENTES .
MANIFESTAÇÃO PELO CONHECIMENTO E PROVIMENTO DO RECURSO ORDINÁRIO.
É o relatório.
RECURSO EM HABEAS CORPUS Nº 89.981 - MG (2017/0250966-3)
VOTO
O EXMO. SR. MINISTRO REYNALDO SOARES DA FONSECA (Relator):
Busca-se, no presente recurso, seja declarada ilícita as provas obtidas pela Polícia Militar, uma vez que na abordagem policial houve violação do conteúdo das mensagens constantes de aplicativo de whatsapp obtidas sem autorização judicial e sem a autorização do acusado, o que feriu a intimidade do recorrente.
Foi a questão assim decidida no Tribunal de origem (e-STJ fls. 116/120):

Analisando os argumentos despendidos no presente writ, verifica-se que a impetração alega suposto constrangimento ilegal tendo em vista que "os Policiais Militares realizaram devassa no aparelho de telefonia celular de um corréu sem autorização judicial para tanto".
Pretendem a concessão da presente ordem para declarar a nulidade das provas colhidas nos autos.
Contudo, o presente writ, tecnicamente, não é o instrumento adequado para valoração do mérito da própria ação penal, por exigir exame aprofundado da prova, a não ser diante da possibilidade de lesão ou ameaça de lesão à liberdade ambulatorial do paciente, nos termos do art. 50, LXVIII da Constituição Federal, o que não se vislumbra no presente caso.
Além disso, conforme se observa da decisão de fls.09/11- TJ, a tese de nulidade foi arguida na resposta à acusação e rechaçada pelo magistrado a quo, senão vejamos:
"(...) Outrossim, infundada a tese de nulidade da prova obtida através do acesso imediato ao aplicativo mensageiro Whastapp do aparelho celular dos denunciados sem autorização judicial.
Isto porque, não obstante a privacidade, intimidade e o sigilo das comunicações telefônicas encontrem-se constitucionalmente assegurados (art. 5°, X e XII, da CF/88), o acesso aos dados constantes em aparelho celular regularmente apreendido pelos policiais na sequência de uma prisão em flagrante caracteriza-se hipótese de exame em instrumento utilizado na prática de crime, constituindo corpo de delito, sendo legítima sua apreensão e análise, a fim de constatar os vestígios da infração. Aliás, o Código de Processo Penal, em seu art. 6°, determina a apreensão imediata de todos os objetos que tenham relação com o fato, bem como de todas as provas que servirem ao seu esclarecimento. E dever do agente proceder de tal modo, o que, no caso dos celulares, significa extrair os dados neles constantes, independentemente de autorização judicial, a fim de saber se possuem alguma relação com a ocorrência investigada.
Além disso, há evidente elemento de urgência no acesso aos aparelhos, já que a demora decorrente da obtenção de um mandado judicial pode trazer prejuízos concretos à investigação, notadamente pela possibilidade de que, em poucos segundos, todos os dados constantes do dispositivo sejam apagados remotamente por qualquer pessoa com acesso à conta do titular. Assim, exigir que o aparelho celular seja primeiramente apreendido, e apenas posteriormente requerida e obtida judicialmente a quebra do sigilo do conteúdo nele armazenado, resultaria na inutilidade da diligência, porque certamente os dados não mais existirão.
Registra-se, ademais, que não se tratou propriamente de devassa aos dados constantes dos aparelhos apreendidos, já que somente o aplicativo mensageiro whatsapp foi examinado. Situação diversa seria o exame aprofundado de outras funções do aparelho, como a tentativa de recuperação de mensagens já apagadas, o acesso à localização para descobrir os últimos locais frequentados etc, que poderiam justificar eventual necessidade de autorização judicial.
Destarte, tratando-se de prisão em flagrante que seguiu o delineado pelo Art. 304 e seguintes do CPP, inexistindo qualquer irregularidade, bem como constatado que o acesso aos dados do aparelho celular foi realizado

imediatamente após o flagrante, para servir efetivamente aos propósitos da persecução penal, visando especialmente preservar os elementos probatórios, inexiste nulidade a ser declarada, afigurando-se lícitas as provas colhidas, (...)"
Neste sentido já se pronunciou este Tribunal:
"EMENTA: HABEAS CORPUS - TRÁFICO LICITO DE ENTORPECENTES E POSSE IRREGULAR DE ARMA DE FOGO - 1RREGULARIDADES DO FLAGRANTE - CONVERSÃO EM PRISÃO PREVENTIVA - MODIFICAÇÃO DO TÍTULO PRISIONAL - ACESSO AO CONTEÚDO DE MÍDIA DO APARELHO CELULAR - DESNECESSIDADE DE AUTORIZAÇÃO JUDICIAL - PROVA LÍCITA - HIPÓTESE QUE NÃO CARACTERIZA INTERCEPTAÇÃO TELEFÔNICA - PRISÃO PREVENTIVA DECRETADA - DECISÃO FUNDAMENTADA- PRESENÇA DOS PRESSUPOSTOS E REQUISITOS DOS ART. 312E SEGUINTES DO CPP - GARANTIA DA ORDEM PÚBLICA - QUANTIDADE RELEVANTE DE DROGAS APREENDIDAS E INDÍCIOS DE REITERAÇÃO DELITIVA - PERSPECTIVA DA REPRIMENDA IN CONCRETO - FIXAÇÃO DE REGIME MAIS BRANDO E SUBSTITUIÇÃO DE PENA - IMPROBABILIDADE - DESPROPORCIONALIDADE DA SEGREGAÇÃO NÃO EVIDENCIADA - CONDIÇÕES PESSOAIS FAVORÁVEIS - IRRELEVÂNCIA - AUSENCIA DE CONSTRANGIMENTO ILEGAL - DENEGADO O HABEAS
CORPUS. (...) - A garantia constitucional de inviolabilidade das comunicações telefônicas diz respeito à vedação de escutas clandestinas, a qual não se confunde com a mera checagem de textos, mensagens ou imagens do celular apreendido. (...)" (Habeas Corpus Criminal 1.0000.17.023709-3/000, Relator(a): Des.(a) Jaubert Carneiro Jaques, Data de Julgamento 18/04/2017, Data da Publicação 04/05/2017)
"EMENTA: HABEAS CORPUS - TRÁFICO DE DROGAS - DESENTRANHAMENTO DE PROVAS ILÍCITAS - SIGILO DE ARQUIVOS ELETRÔNICOS ESTÁTICOS - INAPLICABILIDADE - TRANCAMENTO DA AÇÃO PENAL - IMPOSSIBILIDADE - CONSTRANGIMENTO ILEGAL NÃO CONFIGURADO - ORDEM DENEGADA. A salvaguarda Constitucional do sigilo das comunicações não acoberta direito à prática de ilícito criminal, nem diz respeito à dados armazenados em aparelhos que foram utilizados na execução de crimes. Se forem atendidas as exigências previstas na Lei n° 9.296/96 não há nulidade da prova produzida em decorrência de interceptação telefônica." (...) (Habeas Corpus Criminal 1.0000.16.086709-9/000, Relator (a): Des. (a) Fernando Caldeira Brant, Data de Julgamento 0810312017, Data da Publicação 15/03/2017)
Assim, ausente manifesto constrangimento ilegal sanável de oficio, DENEGO A ORDEM.
Envie-se, imediatamente, cópia desta decisão para ser juntada ao respectivo processo (art. 461 do RITJMG).
Com efeito, a situação retratada nos autos não se encontra albergada pelo comando do art. 5º, inciso XII, da Constituição Federal, o qual assegura a inviolabilidade das comunicações, ressalvando a possibilidade de quebra de sigilo telefônico, por ordem judicial, nas hipóteses e na forma estabelecida pela Lei n. 9.296/1996, para fins de investigação criminal ou instrução processual penal.
Note-se que não foram interceptadas as comunicações telefônicas, nem mesmo as mensagens armazenadas no aparelho celular dos acusados, razão pela qual não há se falar igualmente em inobservância do art. 7º, incisos II e III, da Lei n. 12.965/2014, a qual estabelece os princípios, garantias e deveres para uso da internet no Brasil.
A propósito, transcrevo a norma acima referida:
Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I – (...).
II - inviolabilidade e sigilo do fluxo de suas comunicações pela
internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
(...).
Contudo, embora a situação retratada nos autos não esteja protegida pela Lei n. 9.296/1996 nem pela Lei n. 12.965/2014, haja vista não se tratar de quebra sigilo telefônico por meio de interceptação ou de acesso a mensagens de texto armazenadas, ou seja, embora não se trate violação da garantia de inviolabilidade das comunicações, prevista no art. 5º, inciso XII, da Constituição Federal, houve sim violação dos dados armazenados no celular de um dos acusados.
De fato, deveria a autoridade policial, após a apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados armazenados, haja vista garantia, igualmente constitucional, à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, prevista no art. 5º, inciso X, da Constituição Federal.
Ao ensejo:

PROCESSO PENAL. HABEAS CORPUS. ROUBO MAJORADO. (1) IMPETRAÇÃOCOMO SUCEDÂNEO RECURSAL. IMPROPRIEDADE DA VIA ELEITA. (2) QUEBRA DO SIGILO TELEFÔNICO. PROVIDÊNCIA QUE NÃO SE CONFUNDE COM A INTERCEPTAÇÃO TELEFÔNICA. MOTIVAÇÃO DA MEDIDA. OCORRÊNCIA. ILEGALIDADADE. NÃO RECONHECIMENTO. 1. No contexto de racionalização do emprego do habeas corpus, mostra-se indevida a sua utilização como sucedâneo recursal. 2. Não se confundem as medidas de quebra de sigilo telefônico com a interceptação de comunicação telefônica, esta última albergada, ademais, pela cláusula de reserva de jurisdição. Daí, não são exigíveis, no contexto da quebra de sigilo de dados, todas as cautelas insertas na Lei 9.296/1996. In casu, o magistrado, em cumprimento do inciso IX do artigo 93 da Constituição da República, motivou a quebra do sigilo de dados, com base na intensa utilização de certo terminal telefônico, havendo a franca possibilidade de se desvendar, com base em dados cadastrais oriundos dos registros de companhia telefônica, a autoria de um quarto agente no concerto delitivo. 3. Ordem não conhecida. (HC 237.006/DF, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA, julgado em 27/06/2014, DJe 04/08/2014)

Assim, a análise dos dados armazenados nas conversas de whatsapp, revela manifesta violação da garantia constitucional à intimidade e à vida privada, razão pela qual se revela imprescindível autorização judicial devidamente motivada, o que nem sequer foi requerido.

A propósito:

PROCESSUAL PENAL. RECURSO ORDINÁRIO EM HABEAS CORPUS. TRÁFICO DE DROGAS E ASSOCIAÇÃO AO TRÁFICO. DADOS ARMAZENADOS NO APARELHO CELULAR. INAPLICABILIDADE DO ART. 5°, XII, DA CONSTITUIÇÃO FEDERAL E DA LEI N. 9.296/96. PROTEÇÃO DAS COMUNICAÇÕES EM FLUXO. DADOS ARMAZENADOS. INFORMAÇÕES RELACIONADAS À VIDA PRIVADA E À INTIMIDADE. INVIOLABILIDADE. ART. 5°, X, DA CARTA MAGNA. ACESSO E UTILIZAÇÃO. NECESSIDADE DE AUTORIZAÇÃO JUDICIAL. INTELIGÊNCIA DO ART. 3° DA LEI N. 9.472/97 E DO ART. 7° DA LEI N. 12.965/14. TELEFONE CELULAR APREENDIDO EM CUMPRIMENTO A ORDEM JUDICIAL DE BUSCA E APREENSÃO. DESNECESSIDADE DE NOVA AUTORIZAÇÃO JUDICIAL PARA ANÁLISE E UTILIZAÇÃO DOS DADOS NELES ARMAZENADOS. RECURSO NÃO PROVIDO.

I - O sigilo a que se refere o art. 5º, XII, da Constituição da República é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados, e não dos dados em si mesmos. Desta forma, a obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei n. 9.296/96.

II - Contudo, os dados armazenados nos aparelhos celulares decorrentes de envio ou recebimento de dados via mensagens SMS, programas ou aplicativos de troca de mensagens (dentre eles o "WhatsApp"), ou mesmo por correio eletrônico, dizem respeito à intimidade e à vida privada do indivíduo, sendo, portanto, invioláveis, no termos do art. 5°, X, da Constituição Federal.

Assim, somente podem ser acessados e utilizados mediante prévia autorização judicial, nos termos do art. 3° da Lei n. 9.472/97 e do art. 7° da Lei n. 12.965/14.

III - A jurisprudência das duas Turmas da Terceira Seção deste Tribunal Superior firmou-se no sentido de ser ilícita a prova obtida diretamente dos dados constantes de aparelho celular, decorrentes de mensagens de textos SMS, conversas por meio de programa ou aplicativos ("WhatsApp"), mensagens enviadas ou recebidas por meio de correio eletrônico, obtidos diretamente pela polícia no

momento do flagrante, sem prévia autorização judicial para análise dos dados armazenados no telefone móvel.

IV - No presente caso, contudo, o aparelho celular foi preendido em cumprimento a ordem judicial que autorizou a busca e apreensão nos endereços ligados aos corréus, tendo a recorrente sido presa em flagrante na ocasião, na posse de uma mochila contendo tabletes de maconha. V - Se ocorreu a busca e apreensão dos aparelhos de telefone celular, não há óbice para se adentrar ao seu conteúdo já armazenado, porquanto necessário ao deslinde do feito, sendo prescindível nova autorização judicial para análise e utilização dos dados neles armazenados.

Recurso ordinário não provido.

(RHC 77.232/SC, Rel. Ministro FELIX FISCHER, QUINTA TURMA, julgado em 03/10/2017, DJe 16/10/2017)

PENAL E PROCESSO PENAL. RECURSO EM HABEAS CORPUS. TRÁFICO DE DROGAS. APARELHO TELEFÔNICO APREENDIDO. VISTORIA REALIZADA PELA AUTORIDADE POLICIAL SEM AUTORIZAÇÃO JUDICIAL OU DO PRÓPRIO INVESTIGADO. VERIFICAÇÃO DE MENSAGENS

ARQUIVADAS. VIOLAÇÃO DA INTIMIDADE. PROVA ILÍCITA. ART. 157 DO CPP. RECURSO EM HABEAS CORPUS PROVIDO.
1. Embora a situação retratada nos autos não esteja protegida pela Lei n. 9.296/1996 nem pela Lei n. 12.965/2014, haja vista não se tratar de quebra sigilo telefônico por meio de interceptação telefônica, ou seja, embora não se trate violação da garantia de inviolabilidade das comunicações, prevista no art. 5º, inciso XII, da CF, houve sim violação dos dados armazenados no celular do recorrente (mensagens de texto arquivadas). 2. No caso, deveria a autoridade policial, após a apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados armazenados, haja vista a garantia, igualmente constitucional, à inviolabilidade da intimidade e da vida privada, prevista no art. 5º, inciso X, da CF. Dessa forma, a análise dos dados telefônicos constante do aparelho do recorrente, sem sua prévia autorização ou de prévia autorização judicial devidamente motivada, revela a ilicitude da prova, nos termos do art. 157 do CPP.
3. Recurso em habeas corpus provido, para reconhecer a ilicitude da colheita de dados do aparelho telefônico do recorrente, sem autorização judicial, devendo mencionadas provas, bem como as derivadas, serem desentranhadas dos autos.
(RHC 78.747/RS, Rel. Ministro REYNALDO SOARES DA FONSECA, QUINTA TURMA, julgado em 01/06/2017, DJe 09/06/2017)
Nesse encadeamento de ideias, verifica-se que a obtenção dos dados telefônicos do recorrente e dos corréus se deu em violação de normas constitucionais e legais, a revelar a inadmissibilidade da prova, nos termos do art. 157, caput, do Código de Processo Penal. Dessarte, referidas provas devem ser desentranhadas dos autos, bem como as provas derivadas, cabendo ao Magistrado de origem analisar a nexo de causalidade e eventual existência de fonte independente, nos termos do art. 157, § 1º, do Código de Processo Penal.
Nesse sentido:
A corroborar a validade das demais provas contidas nos autos, e que dão sustentação à peça vestibular e ao édito repressivo, o § 1º do artigo 157 do Código de Processo Penal, com a redação dada pela Lei 11.690/2008, excepciona, em matéria de provas ilícitas, a adoção da teoria dos frutos da árvore envenenada quando os demais elementos probatórios não estiverem vinculados àquele cuja ilicitude foi reconhecida. (HC 117.437/AP, Rel. Ministro JORGE MUSSI, QUINTA TURMA, julgado em 04/10/2011, DJe 20/10/2011)

Ante o exposto, dou provimento ao recurso ordinário em habeas corpus, para reconhecer a ilicitude da colheita de dados dos aparelhos telefônicos (conversas de whatsapp), sem autorização judicial, devendo mencionadas provas, bem como as derivadas, serem desentranhadas dos autos.
É como voto.
Ministro REYNALDO SOARES DA FONSECA
Relator
CERTIDÃO DE JULGAMENTO QUINTA TURMA
Número Registro: 2017/0250966-3 PROCESSO ELETRÔNICO RHC 89.981 / MG
MATÉRIA CRIMINAL
Números Origem: 00653831920168130456 05613449220178130000 10000170561344000 10000170561344001
EM MESA JULGADO: 05/12/2017
Relator
Exmo. Sr. Ministro REYNALDO SOARES DA FONSECA
Presidente da Sessão
Exmo. Sr. Ministro REYNALDO SOARES DA FONSECA
Subprocuradora-Geral da República
Exma. Sra. Dra. MARIA IRANEIDE OLINDA SANTORO FACCHINI
Secretário
Me. MARCELO PEREIRA CRUVINEL

AUTUAÇÃO
RECORRENTE : JUNIO GUEDES FERREIRA
ADVOGADOS : GUILHERME RIBEIRO GRIMALDI E OUTRO(S) - MG129232 JULIO CESAR BATISTA SILVA - MG085191

RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS CORRÉU : WASHINGTON LEITE DE PAULA
CORRÉU : LEIDIVAN DE SOUZA COELHO
CORRÉU : EMERSON JORGE LEITE
ASSUNTO: DIREITO PENAL - Crimes contra o Patrimônio - Furto Qualificado
CERTIDÃO
Certifico que a egrégia QUINTA TURMA, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:
"A Turma, por unanimidade, deu provimento ao recurso, nos termos do voto do Sr.
Ministro Relator."
Os Srs. Ministros Ribeiro Dantas, Joel Ilan Paciornik e Jorge Mussi votaram com o Sr.
Ministro Relator.
Ausente, justificadamente, o Sr. Ministro Felix Fischer.
Ainda neste sentido:
Na ocorrência de autuação de crime em flagrante, ainda que seja dispensável ordem judicial para a apreensão de telefone celular, as mensagens armazenadas no aparelho estão protegidas pelo sigilo telefônico, que compreende igualmente a transmissão, recepção ou emissão de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza, por meio de telefonia fixa ou móvel ou, ainda, por meio de sistemas de informática e telemática. STJ. 5ª Turma. RHC 67.379-RN, Rel. Min. Ribeiro Dantas, julgado em 20/10/2016 (Info 593).

Sem prévia autorização judicial, são nulas as provas obtidas pela polícia por meio da extração de dados e de conversas registradas no whatsapp presentes no celular do suposto autor de fato delituoso, ainda que o aparelho tenha sido apreendido no momento da prisão em flagrante. STJ. 6ª Turma. RHC 51.531-RO, Rel. Min. Nefi Cordeiro, julgado em 19/4/2016 (Info 583).
No Brasil, temos, em sentido contrário, decisão do Superior Tribunal de Justiça, na famosa Operação Lava-jato no seguinte sentido:
Ementa Ofcial
PROCESSUAL PENAL. OPERAÇÃO "LAVA-JATO". MANDADO DE BUSCA E APREENSÃO. APREENSÃO DE APARELHOS DE TELEFONE CELULAR. LEI 9296/96.
OFENSA AO ART. 5º, XII, DA CONSTITUIÇÃO FEDERAL. INOCORRÊNCIA.
DECISÃO FUNDAMENTADA QUE NÃO SE SUBORDINA AOS DITAMES DA LEI 9296/96. ACESSO AO CONTEÚDO DE MENSAGENS ARQUIVADAS NO APARELHO.
POSSIBILIDADE. LICITUDE DA PROVA. RECURSO DESPROVIDO.
I - A obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei 9296/96.
II - O acesso ao conteúdo armazenado em telefone celular ou smartphone, quando determinada judicialmente a busca e apreensão destes aparelhos, não ofende o art. 5º, inciso XII, da Constituição da República, porquanto o sigilo a que se refere o aludido preceito constitucional é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados, e não dos dados em si mesmos.
III - Não há nulidade quando a decisão que determina a busca e apreensão está su cientemente fundamentada, como ocorre na espécie.
IV - Na pressuposição da ordem de apreensão de aparelho celular ou smartphone está o acesso aos dados que neles estejam armazenados, sob pena de a busca e apreensão resultar em medida írrita, dado que o aparelho desprovido de conteúdo simplesmente não ostenta virtualidade de ser utilizado como prova criminal.
V - Hipótese em que, demais disso, a decisão judicial expressamente determinou o acesso aos dados armazenados nos aparelhos eventualmente apreendidos, robustecendo o alvitre quanto à licitude da prova.
Recurso desprovido.
(RHC 75.800/PR, Rel. Ministro FELIX FISCHER, QUINTA TURMA, julgado em 15/09/2016, DJe 26/09/2016)

A decisão no caso *Virginia vs. Baust* em permitir que o acusado não forneça a sua senha pessoal para desbloquear seu *smartphone* é de suma importância, primeiro porque reafirma, de forma clara e incisiva o direito à privacidade, segundo, porque consagra, de forma inequívoca o direito ao silêncio.

A privacidade é regida pelo princípio da exclusividade, cujas atributos são a solidão (o estar só), o segredo, a autonomia. Na intimidade protege-se o estar só, na vida privada, o segredo. A privacidade tem, pois, a ver com a inviolabilidade do sigilo. Ela, como direito, tem por conteúdo a violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão.[46]

Assim, o acesso a dados pessoais no celular é capaz de gerar uma narrativa extensa e perigosa acerca de um indivíduo. Dessa forma, na medida em que a intimidade está relacionada à personalidade do indivíduo, na sua capacidade de livremente desenvolver seu senso crítico e de autodeterminação, o celular não pode ser divorciado do princípio da intimidade.

O conteúdo de um celular revela não só informações íntimas de seu possuidor, mas também de terceiros. Além disso, o celular não deve ser compreendido como mero receptáculo de dados pessoais, mas também como uma tecnologia que efetivamente altera as formas de ser na sociedade, relacionando-se de maneira próxima com a personalidade, esta devendo ser compreendida como objeto de proteção da intimidade.

O acesso a celulares em decisões judiciais paradigmáticas no HC 91.867/PA, de relatoria do ministro Gilmar Mendes, foi decidido que não violava o princípio da intimidade o fato de o policial acessar a lista de telefones no celular de um indivíduo. A referida decisão é eventualmente utilizada como precedente para que policiais possam acessar dados em celulares.

---

[46] FERRAZ JÚNIOR, Tércio Sampaio*. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Cadernos de Direito Tributário e Finanças Públicas, nº 1, São Paulo: RT, 1992. p. 141-154

O uso do precedente como uma permissão para o acesso a outros dados pessoais no celular é equivocado, pois ultrapassa os limites da decisão. Além disso, o uso do precedente decorre de uma má interpretação, uma vez que, no caso, o ministro fez a pergunta se o acesso à lista telefônica seria uma violação da intimidade. Por concluir que não, houve a manutenção da licitude da medida policial.

Aplicando-se devidamente o precedente, parece mais adequado fazer-se o questionamento, caso a caso, se o acesso a determinado dado pessoal no celular estaria ou não violando a intimidade.

Mais coerente com o contexto tecnológico atual se deu a decisão no RHC/RO 51.531, de relatoria do Ministro Nefi Cordeiro, STJ, que declarou ilícita prova produzida em decorrência de acesso a dados no celular sem autorização judicial:
Atualmente, o celular deixou de ser apenas um instrumento de conversação pela voz à longa distância, permitindo, diante do avanço tecnológico, o acesso de múltiplas funções, incluindo, no caso, a verificação da correspondência eletrônica, de mensagens e de outros aplicativos que possibilitam a comunicação por meio de troca de dados de forma similar à telefonia convencional.

Deste modo, ilícita é tanto a devassa de dados, como das conversas de whatsapp obtidos de celular apreendido, porquanto realizada sem ordem judicial.

Cabe registrar que o Poder Público tem limites frente aos direitos e garantias fundamentais do indivíduo, não podendo, desta forma, atingir a liberdade de cada um valendo-se do arbítrio e em confronto direto com o direito. [47]

Conforme Leonardo Costa de Paulo[48] “todavia, cumpre proceder a análise distinta, já que, em um Estado Democrático de Direito, a preocupação no processo penal consiste

[47] Garcia, Rafael de Deus, Acesso a dados em celular exige autorização judicial, Revista Consultor Jurídico, 6 de fevereiro de 2017.

em não só aplicar a lei ao caso concreto, mas especificamente, pensar que é o locus ideal para a preservação das garantias constitucionais do réu."

Situações semelhantes já foram objeto de exame pelas Cortes Americanas que chegaram a resultados distintos em *US vs. Fricosu e US vs. Doe*, citados por Nicholas Soares em artigo publicado na *American Law Review: Direito de Permanecer Criptografado: A Doutrina da autoincriminação na Era Digital Penal*. O autor, em seu artigo demonstra grande preocupação de os tribunais lidarem com um assunto que envolve tecnologia moderna e sua incapacidade de prover justiça.

Este risco não se coloca a partir de uma fonte externa, nem de um desacordo nascente com os valores inerentes a esse princípio. Pelo contrário, a proteção contra a autoincriminação, direito garantido pela Quinta Emenda, está em perigo em face de uma doutrina míope e inflexível adotada por uma Suprema Corte que parece ter perdido de vista os princípios subjacentes garantidores da emenda, uma doutrina que está doente, inadequada para lidar com os avanços tecnológicos em áreas como a criptografia.[49]

No direito americano, bem como na grande maioria da doutrina estrangeira o direito ao silêncio (*right to remain silence*) só é plenamente exercido quando envolve compulsão de ordem testemunhal, ou seja, é assegurado o direito ao acusado de calar-se quando suas declarações podem ser interpretadas em seu desfavor.

Em *United States vs. Kirshner* a Suprema Corte Americana citando a decisão do Supremo Tribunal em *Doe II*, afirmou que "é extorsão de informações do acusado, a tentativa de forçá-lo a divulgar o conteúdo de sua própria mente", o que implica em autoincriminação. Ao contrário de uma amostra escrita à mão ou um exemplar de voz,

---

[48] PAULO, Leonardo Costa de*. Autoincriminação e ilicitude na obtenção da prova –A limitação do poder*. Revista Eletrônica de direito processual. Vol.4., 2009. Disponível em:< http://www.arcos.org.br/periodicos/revista-eletronica-de-direito-processual/volume-iv/auto- incriminacaoe-ilicitude-na-obtencao-da-prova-a-limitacao-do-poder>

[49] SOARES, Nicholas. *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age.* American Criminal Law Review, vol. 49, nº4, 2012.(tradução livre)

uma intimação exigindo que o arguido revele a senha do seu computador se comunica "conhecimento" concluindo que a cláusula de autoincriminação o protege de divulgar, através de seus processos mentais a senha de seu computador.[50]

Assim, a determinação crucial para um tribunal é se inserir uma senha de computador constitui um depoimento. A pedra de toque de saber se um ato de produção é testemunhal é se o governo obriga o indivíduo a usar o conteúdo de sua própria mente para explícita ou implicitamente comunicar alguma declaração de fato." Em outras palavras, um ato de produção não é testemunhal se apenas obriga o requerido a fazer alguma ação ou omissão física que não requeira o uso do conteúdo de sua mente, ou onde a existência, a posse, ou a autenticidade do conteúdo são uma precipitada conclusão. A inserção de uma senha ou outra forma de descriptografar o conteúdo em um computador ou smartphone é um ato testemunhal que recebe a proteção integral da Quinta Emenda, ou de qualquer direito ou garantia fundamental baseados no *nemo tenetur se detegere*.

A Suprema Corte distinguiu atos testemunhais e não testemunhais comparando a combinação de um cofre com a sua chave. A combinação envolve o conhecimento da mente, é íntimo, pode ser “esquecido”, já a entrega de uma chave é um fazer, não implica em testemunho, mas mero ato físico, com amparo legal.

O que se protege, *in casu,* é o conhecimento pessoal de informação que possa prejudicar o acusado, é a própria razão de ser do *nemo tenetur se detegere* a se aceitar outra interpretação é aceitar o fim do direito ao silêncio, do direito a não se auto incriminar, já tão diluído pela doutrina e pela jurisprudência!

Tal direito pode ser exercido em qualquer fase, seja judicial ou extrajudicial.

---

[50] Idem. (tradução livre)

A doutrina e a jurisprudência americanas, de forma restritiva entendem que o direito ao silêncio só é válido em relação às declarações do acusado que envolvam manifestação verbal ou por escrito.

Mesmo não tendo o mesmo conteúdo, o direito ao silêncio e a garantia a não autoincriminação, no dizer de Jorge Figueiredo Dias e Manuel da Costa Andrade, "estão incidivelmente ligados: não lhe sendo reconhecido o direito a manter-se em silêncio, o arguido seria obrigado a pronunciar-se revelando informações que o podem eventualmente prejudicar na medida em que contribuem para a sua condenação".[51]

8- Da Relativização do Direito ao Silêncio

Este direito, hoje em dia, encontra-se cada vez mais ameaçado pelas circunstâncias da modernidade.

Segundo o magistério de Sofia Lara Pinto, para aferir da extensão do princípio *nemo tenetur* é preciso verificar a extensão das suas componentes (o privilégio contra a autoincriminação e o direito ao silêncio), sendo que este terá a extensão que as suas componentes tiverem. Devemos verificar o âmbito dos vectores do princípio *nemo tenetur*, abordando o problema da delimitação do direito ao silêncio em relação ao privilégio contra a autoincriminação. A referida delimitação problemática entre o direito ao silêncio e o privilégio contra a autoincriminação resulta do facto de ser recorrente falar-se indistintamente do direito ao silêncio e do privilégio contra a autoincriminação, sendo que, aquele, está contido neste, não resultando claro qual o âmbito de aplicação de um ou de outro; ou até se são expressões equivalentes, traduzindo a mesma realidade e tendo o mesmo campo de aplicação. Mais, em conformidade com a lição de VÂNIA COSTA RAMOS que a doutrina é consensual em admitir que o direito ao silêncio cobre outras formas de cooperação autoincriminatória que não apenas as declarações do arguido, e «no entanto, continua a fazer-se uso da expressão direito ao silêncio em homenagem ao seu aparecimento e evolução históricas (...)». Observando

[51] DIAS, Jorge de Figueiredo. Andrade, Manuel do Costa. *Supervisão, Direito ao Silêncio e legalidade da prova*. Ed. Almedina. 1ª ed. 2009. P. 38

o direito ao silêncio na sua consagração legal, diz-nos o art. 61.º/1d) CPP que o direito ao silêncio abrange as declarações sobre os factos típicos que lhe são imputados. Mas são discutidas na doutrina duas extensões possíveis do direito ao silêncio: (i) Uma extensão minimalista, incidindo apenas sobre as declarações do arguido em sentido estrito (prova por declarações) e sobre os factos que lhe são imputados. (ii) Ou uma extensão maximalista, abarcando as declarações por meio de documentos, da indicação do lugar onde se encontra o meio de prova, de uma atuação, consubstanciando-se num direito a não ser obrigado a fornecer prova (documental, declaracional ou outra) da sua culpabilidade. Perante este cenário, temos para nós que há que separar as águas, impondo-se fazer um ponto de situação sobre o âmbito de aplicação destes dois vectores, sob pena de contribuir para a manutenção do limbo existente nesta matéria. Pela nossa parte, cremos que deve entender-se que a área de aplicação do privilégio contra a autoincriminação e do direito ao silêncio deve ser configurada da seguinte forma: O privilégio contra a autoincriminação traduz-se no direito a não cooperar no fornecimento de quaisquer meios de prova para a sua incriminação (sentido amplo). Este corresponde ao entendimento originário do privilégio, tendo já sido pormenorizado anteriormente. A jurisprudência do TEDH confirma a extensão do privilégio nestes termos, bem como a parca jurisprudência do STJ encontrada. Por sua vez o direito ao silêncio apenas abarca a colaboração do arguido na sua incriminação através de declarações sobre os factos que lhe são imputados. Portanto apenas está aqui em causa o meio de prova por declarações. O acórdão do TC n.º 372/98 já veio associar o direito ao silêncio à norma do art. 61.º/1d) CPP, pelo que se confirma este entendimento quanto ao seu âmbito. Entendemos que o privilégio contra a autoincriminação abrangeria, em abstrato, o direito ao silêncio no seu âmbito de aplicação (sentido estrito), uma vez que o privilégio abarca toda e qualquer colaboração na sua incriminação, mas devido à especificidade de se tratar de um meio de prova por declarações, ganha uma certa autonomia, ficando numa relação de especialidade face ao privilégio contra a autoincriminação. Definida a extensão das componentes do princípio *nemo tenetur*, deve ainda notar-se que nenhuma destas é absoluta, admitindo-se a possibilidade de derrogações pontuais pela lei.[52].

---

[52] Pinto, Sofia Lara, PRIVILÉGIO CONTRA A AUTO-INCRIMINAÇÃO VERSUS COLABORAÇÃO DO

Jorge de Figueiredo Dias e Manuel da Costa Andrade entendem que o direito ao silêncio e a não se autoincriminar deverá ser sempre aplicado quando expuser a pessoa ao risco de ser penalmente perseguido. Embora a aplicação extensa de tais direitos não signifique que eles tenham um caráter absoluto, podendo, em determinadas circunstâncias, serem restringidos. E exemplificam tais limitações no ordenamento português:

- o direito ao silêncio não se aplica ao arguido relativamente a perguntas sobre sua identidade, na forma do artigo 61º, nº 3, al. b\0 do CPP;
- a obrigatoriedade de realizar determinados exames.

Entre outros, sendo que o que nos interessa, *in casu*, é o primeiro exemplo.

Prosseguem ainda os renomados juristas no sentido de que, dada a natureza constitucional destes direitos, estas restrições devem obedecer a dois pressupostos:

- Devem estar previstas em lei prévia e expressa, de forma a respeitar a exigência de legalidade:
- Devem também obedecer ao princípio da proporcionalidade e da necessidade, previsto no artigo 18º, nº 2, da CRP.[53]

O princípio da necessidade se refere à utilização do meio que menos interfira em um direito fundamental, sem entrar na questão da adequação entre meios e fins. Por exemplo, se podemos conseguir as provas por meio de provas testemunhais, por que

---

ARGUIDO Case study: revelação coactiva da password para desencriptação de dados – resistance is futile?- PROVA CRIMINAL E DIREITO DE DEFESA Estudos sobre teoria da prova e garantias de defesa em processo penal AUTORES ANA RITA FIDALGO • EURICO BALBINO DUARTE • FÁBIO LOUREIROLARA SOFIA PINTO • LUÍS PEDRO MARTINS DE OLIVEIRA • NUNO SERRÃO DE FARIARITA SERRANO • SANDRA PEREIRA • SOFIA SARAIVA DE MENEZES COORDENADORES TERESA PIZARRO BELEZA FREDERICO DE LACERDA, Editora Almedina, 2ª reimpressão, 2013.

[53] DIAS, Jorge de Figueiredo. Andrade, Manuel do Costa. Supervisão, Direito ao Silêncio e legalidade da prova. Ed. Almedina. 1ª ed. 2009. Pp. 38/39.

violar a intimidade do réu com uma interceptação telefônica? Por que decretar prisão preventiva, com fundamento na conveniência da instrução criminal, supondo que o réu destruiria documentos comprometedores, se bastam a busca e a apreensão para resguardá-los?

No princípio da proporcionalidade em sentido estrito (ou subprincípio da proporcionalidade), temos:

a) O que colide: de um lado, direitos fundamentais afetados e, de outro, "princípios" (objetivos, princípios, direitos, deveres, garantias, interesses e bens constitucionais);

b) Método de resolução da colisão: a ponderação;

c) Valor dos entes colidentes: os pesos argumentativos presuntivos, que demandam a apresentação de contra-argumentos para os argumentos ou razões favorecidas com as presunções;

d) Circunstâncias da colisão e da ponderação: circunstâncias do caso concreto;

e) Resultado da colisão e da ponderação: "relação de precedência condicionada" às circunstâncias do caso concreto, mediante a qual as condições ou circunstâncias sob as quais um "princípio" precede a outro constituem o suposto de fato de uma regra que expressa a consequência jurídica do princípio prevalecente.

Por aplicação do princípio da proporcionalidade em sentido estrito, mesmo estando presentes, por exemplo, os "requisitos" ou pressupostos legais lato sensu para decretação da prisão preventiva, ela pode deixar de ser decretada pelo juiz.[54]

---

[54] Pacheco, Denilson Feitoza, Princípio da proporcionalidade no direito processual penal, http://www.cartaforense.com.br/conteudo/artigos/principio-da-proporcionalidade-no-direito-processual-penal/4208.

Presentes estes requisitos, sendo que o segundo exige uma apreciação concreta da natureza dos conflitos em causa estas restrições deverão ser consideradas constitucionais mesmo em matéria criminal.[55]/[56]

9 – A contribuição do terrorismo global para a relativização do direito ao silêncio

Muitos autores, sobretudo de países que convivem com a ameaça do terrorismo, já constroem manifestações no sentido de se possibilitar a extração de informações de suspeitos da prática ou possível prática de atos terroristas através de tortura, narcóticos, hipnose, etc. Estas manifestações encontram guarita na população temerosa que vê, através da imprensa, os horrores que são praticados por grupos com viés político ou religioso.

No mesmo sentido atenua-se o direito ao silêncio nos países onde há aumento de criminalidade, pois onde esta avulta decrescem os direitos individuais do cidadão.[57]

O Parlamento da Grã-Bretanha aprovou a proposta para reduzir significativamente o direito ao silêncio. A nova lei permite que os juízes e jurados considerem como prova

---

[55] JORGE DE FIGUEIREDO DIAS/MANUEL DA COSTA ANDRADE, (Parecer) in Supervisão, direito ao silêncio e legalidade da prova (CMVM) Almedina, Coimbra, 2009, pp. 44/45.

[56] A respeito do art. 61.º/3d) CPP, diz o acórdão Ac. do TRP (Relatora Maria do Carmo Silva Dias) de 01-28-2009 (processo n.º 0816480), «o facto de o arguido dever sujeitar-se a diligências de prova, numa perspectiva eminentemente passiva que ressumbra do próprio termo "sujeitar", não significa que o arguido seja obrigado a colaborar activamente para a descoberta da verdade e para a obtenção de prova incriminadora. Aliás, pelo contrário, atentas as exigíveis garantias de defesa do arguido, na decorrência do seu direito ao silêncio consagrado no art. 32.º, n.º 1 da CRP, no art. 6.º, n.º 2 da CEDH, e no próprio art. 61.º, n.º 1, al. d) do CPPP, conclui-se que não existe qualquer dever de colaboração do arguido, especialmente quando está em causa a sua incriminação». O Tribunal a quo acolhe implicitamente a doutrina tradicional alemã quando afirma que «importa distinguir a exigibilidade da sujeição passiva a diligências de prova, como sejam os reconhecimentos e grande parte dos exames, da exigibilidade de um comportamento activo do arguido, sendo que, enquanto aqueles, pela passividade do comportamento que lhes é inerente, não bulem com o direito do arguido a não contribuir para a sua incriminação, já o mesmo não sucede com as diligências que impliquem uma conduta activa do arguido, como seja, por exemplo, a notificação do arguido para apresentar documentos ou objectos (porventura a arma dilênckoo crime). No caso dos autos, a diligência ordenada ao arguido exigia um comportamento que seria susceptível de contribuir para a sua incriminação, por estava em causa apurar se a imputada falsificação de um escrito teria sido realizada pelo

[57] NUCCI, Guilherme de Souza. *Provas no processo penal*. Ed. Forense. 4ª ed.2015

de culpa quando um suspeito se nega a responder às perguntas da polícia durante os interrogatórios e a recusa do réu a depor durante o julgamento. Os defensores da nova lei argumentam que a mudança era muito necessária porque o direito ao silêncio é "uma farsa que [tem sido] impiedosamente explorado por terroristas".[58]

Os avanços tecnológicos supuseram um passo transcendental, e por um lado inevitável, na investigação policial através do que se denomina tecnovigilância, busca automática na rede, análise de pastas de arquivos, programas de informática para leituras automáticas, vídeo vigilância mediante IP com ativação remota, sistema de imagens aéreas, infravermelhas ou de visão noturna, entre outros programas de informática para a interceptação e gravação, em tempo real, da informação transmitida ou recebida através dos diferentes meios de comunicação etc.[59]

Seu surgimento também no âmbito da criminalidade exige um novo entendimento do conceito de comunicação e do objeto de proteção do direito fundamental que estenda a proteção a estes novos âmbitos... o desenvolvimento foi muito desigual e a discussão atualmente centra-se na admissibilidade de programas espiões como o CIPAV norte americano, ou o on line Durchsuchung alemão.[60]

Alan M. Dershowitz, professor emérito na Universidade de Harvard, e ativista dos direitos civis, assim se manifestou sobre este assunto em matéria publicada no Boston Globe de 18/09/2014, sob o título: A escolha de males: Devem as democracias usar tortura para se protegerem contra o terrorismo? [61]

O autor afirma que, se estiver certo, e se todos os presidentes que, de fato, considerem optar pela tortura de um terrorista, em vez de permitir que milhares de americanos inocentes possam ser explodidos, então a seguinte pergunta deve ser feita: seria

---

[58] O'Reilly, Gregory W. *England Limits the Right to Silence and Moves towards an Inquisitorial System of Justice*. Journal of Criminal Law and Criminology. Vol. 85, No. 2. 1994

[59] Deu, Teresa Armenta. A prova ilícita- um estudo comparado.1.ed, São Paulo: Marcial Pons, 2014.

[60] idem

[61] Boston Globe de 18/09/2014

melhor ou pior uma lei a ser aprovada que exige que o presidente para garantir tal situação obtenha um mandado antes (ou, em uma emergência real, durante ou logo após) que lhe permita empregar essa medida drástica? Tal lei legitimaria a tortura em situações extremas, e isso é um fato abominável, mas também criaria a visibilidade e a responsabilidade, o que seria mais aceitável.

Mais uma vez, somos confrontados com uma escolha terrível: dos males, o menor.

Dershowitz manifesta seu desejo de que ninguém jamais venha a torturar, mas tem a certeza que alguns terão vontade, se a situação emergencial surgir. É por isso que se manifestou, no passado, a favor de mandados de tortura.

A tortura mina os alicerces do Estado de Direito convertendo-o paulatina e irreversivelmente num Estado de não Direito. Esta metamorfose não se mitiga pelo fato de a tortura ser prevista na lei e controlada pelos tribunais, antes é, num certo sentido, acelerada e acentuada por isso.

A legalização da tortura representa um regresso ao modelo inquisitório do processo penal autocrático. Neste modelo, o arguido é concebido desde o início como presumivelmente culpado, destituído de direitos e pleno de deveres, um dos quais é o de colaborar com as autoridades, contribuindo para a descoberta da verdade e, portanto, para a sua eventual autoincriminação.

A fim de assegurar o seu cumprimento coativo, é instituída a tortura e elevada a confissão a rainha das provas. O arguido é, deste modo, coisificado como meio de obtenção da prova e colocado ao dispor dos inquisidores. A presunção de inocência, o direito à não autoincriminação e a sua mais importante realização, o direito ao silêncio, pilares fundamentais de um modelo processual de estrutura acusatória, não fazem qualquer sentido em um tal contexto.

A tortura representa a antítese profunda de qualquer deles. A circunstância de a tortura ser aplicável exclusivamente a indivíduos perigosos, que perderam o estatuto de pessoa por não darem garantia cognitiva de um comportamento fiel ao Direito, não altera as coisas pois só por ingenuidade ou má fé se pode pensar que o sistema constitucional dos direitos e garantias não é válido para estes, nem manchado por uma tal lógica de exceção. A dignidade da pessoa e a titularidade de direitos e liberdades fundamentais não dependem de um status ou de um comportamento social. [62]

A Declaração Universal dos Direitos do Homem (art. 5º), o Pacto Internacional dos direitos civis e políticos (art. 7º), a Convenção contra a tortura e outras penas ou tratamentos cruéis, desumanos ou degradantes, ratificados por Portugal em 1988, a Carta de direitos fundamentais da União Europeia (art. 4º), a que se junta a Constituição da República Portuguesa (CRP) (art. 25º nº 2), proíbem a tortura de uma forma peremptória. Poucas são as práticas tão consensual e redondamente proibidas quanto a tortura. A tortura é universalmente considerada um atentado inadmissível à dignidade humana e ao direito das pessoas à integridade pessoal.

Esta valoração justifica decerto que em muitos ordenamentos jurídicos a proibição da tortura assuma carácter penal. O ordenamento jurídico português não constitui excepção. O art. 243º do Código Penal (CP), inserido no Título III da Parte Especial dos crimes contra a identidade cultural e a integridade pessoal, prevê o crime de tortura. Encontramos no nº 3 uma definição segundo a qual «considera-se tortura, tratamento cruel, degradante ou desumano, o acto que consista em infligir sofrimento físico ou psicológico agudo, cansaço físico ou psicológico grave ou no emprego de produtos químicos, drogas ou outros meios, naturais ou artificiais, com intenção de perturbar a capacidade de determinação ou a livre manifestação de vontade da vítima». Do mesmo modo que a CRP e os citados diplomas de Direito Internacional, o CP não distingue entre tortura e tratamento cruel, degradante ou desumano, significando isto que qualquer distinção conceptual que se pretenda fazer não tem correspondência no

[62] Dias, Augusto Silva. *Torturando o inimigo ou libertando da garrafa o gênio do mal? Sobre a tortura em tempos de terror.* Revista do Ministério Público do RS, Porto Alegre, n. 71, jan. 2012 – abr. 2012

plano prático-normativo. Por outro lado, adopta o CP um conceito sufi cientemente amplo para abranger as formas mais camufladas, sofisticadas e «indolores» de tortura e, ainda, para frustrar qualquer diferenciação entre tortura «boa» e tortura «má». Deve entender-se que essa definição de tortura vale para todo o ordenamento jurídico nacional, exceto nos aspectos em que as definições dos diplomas de Direito Internacional citados resultem mais latas. A ratificação pelo Estado português daqueles diplomas de Direito Internacional obriga, por si só, a este entendimento.[63]

É controverso entre os liberais e os conservadores que, no cômputo geral, a visibilidade e a responsabilidade são fundamentais para a democracia, mesmo que isso signifique emprestar alguma legitimidade a uma tática imoral e desprezível como a tortura.

Tal é a natureza e a complexidade do processo de tomada de decisão baseada em princípios ao confrontar os males do terrorismo no Estado de direito. Não há respostas perfeitas, mas algumas são piores que outras. Em tais situações, a responsabilidade democrática sugere que deveríamos geralmente optar pela abordagem que é mais compatível com o Estado de Direito e as realidades do terrorismo.

O problema do direito ao silêncio que deu origem ao presente toma dimensão maior quando transportado para o panorama que se descortina em um mundo globalizado, onde para se ter acesso a todo e qualquer lugar se exige uma senha.

A internet, hoje inerente a todo ser humano, já exige senhas para ingresso em quase todos os sítios. Ela torna possível o anonimato, mas permite, àqueles que desejam e têm conhecimento, bisbilhotar, invadir a privacidade, incriminar, furtar e praticar uma série de atos porque o ser humano, só entre tantos, sente-se tentado a revelar-se perante uma máquina, um smartphone, tal qual estivesse na santidade de um confessionário, não atentando para o risco que traz para si e para as demais pessoas.[64]

---

[63] Idem.
[64] Cf. CONSTABLE, Mariane. *Just silences : the limits and possibilities of modern law*. Princeton University Press. 2005.

Com a internet e os arquivos virtuais tem-se modificação no conteúdo de proteção da norma: antes, a residência sempre fora identificada como local de morada, daí a necessidade de proteção. Mas, agora, será possível estender-se para a proteção da residência a informação que é guardada em arquivos virtuais? Será possível permitir-se o acesso a bancos de dados virtuais sem mandado judicial? Caso haja necessidade, a proteção se dá pelo domicílio ou pela intimidade?[65]

Estes questionamentos ainda não foram adequadamente respondidos pelas cortes internacionais. A Corte Interamericana não apresenta resposta alguma à proteção de dados na internet. Já a Corte Europeia tem dado a resposta de forma insatisfatória: reconhece-se a violação de direito fundamental unicamente pela ausência de legislação que preveja a possibilidade de quebra deste direito. Não há, na Corte Europeia, o estabelecimento de balizas para a identificação dos parâmetros para a quebra da proteção da intimidade.

Tal qual dito no início, a velocidade com que a tecnologia avança, dificulta seu acompanhamento pelo direito. O Congresso Americano tem tentado regulamentar o uso de criptografia através de uma série de projetos de lei (Senadores McCain e Kerrey Bill) bem como diretivas presidenciais, sempre esbarrando nas 4ª e 5ª emendas.

O direito norte americano tem se valido da teoria denominada *foregone conclusion* (conclusão antecipada) onde um ato de produção não é testemunhal - mesmo que este ato transmita um fato relativo à existência ou localização, posse ou autenticidade dos materiais intimados - se o Governo puder mostrar com "razoável particularidade" que, na época em que buscava forçar o ato de produção, já conhecia os materiais, tornando qualquer aspecto testemunhal uma conclusão precipitada.

---

[65] DEZEM, Guilherme Madeira*. A proteção da intimidade e os tribunais internacionais. In: RASCOVSKI, Luis (coord.). Temas relevantes de Direito Penal e Processual Penal.* São Paulo: Saraiva, 2012

Nesta hipótese, o governo já tem conhecimento de que as provas existem no disco rígido, ou smartphone, apenas precisariam da corroboração por parte da divulgação da palavra passe por parte do arguido para "pescar" tais provas.[66]

---

[66] Terzian, Dan. The Micro-Hornbook on the Fifth Amendment and Encryption. https://georgetownlawjournal.org/articles/151/micro-hornbook-fifth-amendment-encryption.
Citation: 104 Geo L.J. Online 168 (2016)
The DOJ calls encryption a "zone of lawlessness."1 Others call it an "[e]scape from [t]yranny."2 Opinions on encryption clearly diverge. But this micro-hornbook isn't about opinions. It's about the law—on what happens when the government has the right to search digital data (perhaps through a search warrant), but can't because the data is password protected and encrypted. Can the government, without violating the Fifth Amendment, force a phone's owner3 to (a) produce the phone's password or (b) produce the decrypted phone (i.e., force her first to enter the password and then to produce the phone)? The first question's answer is easy; the second's answer is hard; and this micro-hornbook sketches the answers for both.

I. Forcing Production of the Password?
Whether the government can force a person to divulge her password depends on the password's type.

Unquestionably, the government can force people to produce bio-metric passwords like fingerprints. The Fifth Amendment does not protect against forced physical acts, such as the taking of fingerprint or voice samples, or even forcing a person "to make a particular gesture."4 For this reason, a Virginia trial court reached the unremarkable conclusion that there is no cellphone exception to the Fifth Amendment.5 So if you use a fingerprint to unlock your phone, the government's right to take fingerprint samples potentially allows it to access your phone.6 Whether it actually allows the government to access your phone depends on the circumstances, as a fingerprint won't unlock an iPhone that's gone untouched for more than 48 hours.7

Almost as certainly, the government can't force you to produce a password.8 The touchstone doctrine here stems from an oft-repeated line of Supreme Court dicta: The government can "force[] [someone] to surrender a key to a strongbox containing incriminating documents," but it can't force him "to reveal the combination to [a] wall safe."9 Because a password is essentially a combination, several courts have held that the government can't force you to produce your password.10

II. Forcing Production of the Decrypted Phone?
The next, and more difficult, question is whether the government can force you to enter the password, which decrypts your phone. There is no right answer here, and you can argue it constitutional or not—unless you're in the Eleventh Circuit or Massachusetts. The former's litigants are bound by the rule that forced decryption is not constitutional, and the latter probably the opposite.11

The arguments trace three fronts: the key—combination dicta just discussed; forced decryption's physicality; and the foregone conclusion exception.

A. The Key—Combination Dicta
The first front stems from the dicta instructing that a key's production can be compelled but a combination's cannot.12 Some courts have extended this dicta to forced decryption. Most notably, the Eleventh Circuit held that forced decryption—which requires the respondent "to use a decryption password"—"is most certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind."13

Yet this extension is questionable. For one thing, the referenced dicta concerns producing a safe's unlocking mechanisms; it's not about producing a safe's contents, which is what forced decryption seeks. For another, safes and encryption differ markedly: the government can always crack a safe; rarely can it

aPara ilustrar o que foi dito, conveniente é mencionar a metáfora proposta por Luiz Flávio Gomes (2002, p. 34). Valendo-se da imagem do elefante e do rato, ele diz que o tradicional direito penal é, em termos de velocidade, um verdadeiro elefante porque se baseia na pena privativa de liberdade e exige consequentemente, o devido processo legal clássico: investigação burocratizada, denúncias, provas, instrução demorada, contraditório, ampla defesa, sentença, recursos, etc. Ao passo que a criminalidade da

---

crack encryption.14 This chasm could persuade a court to disregard the dicta, or at least to apply it less mechanistically.15

B. Forced Decryption's Physicality
The second front is forced decryption's physicality. The government can compel you to perform physical acts, like providing handwriting or voice samples.16 This includes producing a safe's key, assuming the above dicta is binding.

But what about forcing you to enter a password? Is this a compellable physical act? Three courts have answered no.17 In their view, forcing a person to use a password to decrypt a hard drive is not a physical act because it forces the person to "use the contents of his mind."18 Also prevalent in these courts' reasoning is the key—combination dicta already discussed: "A password, like a combination, is in the suspect's mind, and is therefore testimonial . . . ."19

So far, no courts have answered differently. Yet nearly any court (save those in the Eleventh Circuit) could still decide the issue differently because they are not bound by the foregoing cases. And maybe courts should decide it differently because everything—even physical acts—requires minimally using your mind. You can't produce a key unless you remember where you put it. Prosecutors arguing physicality should also challenge these three courts' questionable approach of taking dicta on forcing people to produce unlocking mechanisms and then extending it to the issue of forcing people to use unlocking mechanisms (to produce the de-crypted data itself).

C. The Foregone Conclusion Doctrine
The final front is the "foregone conclusion" doctrine. Even if forced decryption is not a physical act, and even if forced decryption is more like producing a combination than a key, forced decryption is still constitutional if it falls within the foregone conclusion exception.

This exception permits the government to obtain documents that it already knows exist.20 Courts applying the exception to subpoenas for decrypted hard drives have divided on a fundamental issue: what is the document that the government must know of? Is it a particular file, or is it instead the existence of the hard drive's contents generally?

Some courts require that the government know of "a certain file."21 Other courts apparently require only that the government know of the potential for unencrypted files, even if it doesn't know the contents of those files because they're encrypted.22 What's more, the government will always know this whenever it sees an iPhone's password prompt. Thus, the first group of courts allows forced decryption only in the rare instances where the government already knows what's on the hard drive, and the second group allows it virtually always. None of these courts explain their reasoning, or even acknowledge the issue. So lawyers on both sides will need to marshal reasons in favor of one approach and against the other.23

Conclusion
If the government wants a fingerprint, it's getting it. If the government wants a password, it's not getting it. And if the government wants a decrypted hard drive, it may or may not get it.

era pós-industrial, e mais recentemente, da globalização, é velocíssima, tanto quanto os ratos. Impossível, pois, conter o rato (criminalidade organizada) com a lentidão do elefante (direito penal clássico)[67].

Enquanto vivermos num mundo onde uma filosofia de soberania do século XII é reforçada por um modelo judiciário do século XVIII, defendido por um conceito de combate ao crime do século XIX que ainda está tentando chegar a um acordo com a tecnologia do século XX, o século XXI pertencerá aos criminosos. [68]

Conforme se depreende do exposto, temos que, um caso, aparentemente simples, suscita uma série de questionamentos que extrapolam, e muito, sua essência.

As discussões que com certeza terão origem nessa decisão influenciarão o mundo, considerando que a garantia a não autoincriminação, foi com o passar do tempo sendo cada vez mais restringida, restando, praticamente, o direito ao silêncio, sobretudo nos países onde o terrorismo é uma ameaça real e constante como os europeus e os Estados Unidos.

Com a globalização do terror, as autoridades têm buscado alternativas que possam minimizar as ameaças que amedrontam a população, enxergando e teorizando, sob um viés mais permissivo, providências que autorizam um combate mais eficaz as atrocidades que vitimaram suas comunidades.

Somente a partir das duas últimas décadas do século XX, iniciou-se o processo de maior investigação e combate acerca da prática do terrorismo de maneira mais acentuada. Até então, este instituto tinha características mais regionais e menos

---

[67] GOMES, Luiz Flávio. *Crime organizado: que se entende por isso depois da Lei 9.034/95? (Apontamentos sobre a perda da eficácia de grande parte da Lei 9.034/95)*. Disponível em: <http://www.jus.br/doutrina/texto.asp? id=2919>. Acesso em: 25 mar. 2007.

[68] ROBINSON, Jeffrey. *A globalização do crime.* Rio de Janeiro. Ediouro. 2001

cobertura midiática. Era problema de regiões localizadas, tais como o oriente médio e regiões da África, bem como alguns países europeus (tais como Irlanda e Espanha).

Os estudos se intensificaram com o aumento dos ataques terroristas supranacionais que, por sua violência e mudança de cenário chamaram a atenção, não só da imprensa, mas passaram a ser vistos como fenômeno político, sociológico, jurídico e estratégico.

A grande luta era travada entre Judeus e Palestinos, através dos grupos de diversas tendências religiosas e políticas do mundo árabe em sua “guerra” contra o Estado de Israel. “Guerra” esta que ultrapassou as fronteiras do Oriente Médio e o apoio de países ocidentais ao Estado de Israel deslocou o terror para a Europa, chegando aos Estados Unidos da América.

O aumento da sofisticação dos ataques, quer tática, quer tecnologicamente mostrou que o mundo não estava preparado para ações dessa natureza. O perigo do uso de armas de destruição em massa, o cyber terrorismo, bem como o efetivo apoio financeiro de simpatizantes das respectivas causas, aliados ao fanatismo político e, principalmente, religioso tornou o mundo inseguro.
Tal insegurança levou a mobilização dos países na luta global contra o terrorismo. Historicamente, a luta contra o terrorismo internacional teve origem em 1970, em uma assembleia geral da Organização da Aviação Civil Internacional – OACI, convocada por iniciativa da Suíça, que percebeu a necessidade de reprimir com eficácia a ação de sequestradores que praticavam atos de violência contra aeronaves condenando tais ações e iniciando a prevenção e combate a atos criminosos relacionados a aviação.

No mesmo sentido, em 1980 a Agência Internacional para a Energia Atômica incentivou a elaboração da Convenção sobre a Proteção Física de Materiais Nucleares.

Em seguida, com o atentado ao navio Achille Lauro em 1985, a Organização Marítima Internacional - OMI, conseguiu, em 10/03/1988, a aprovação da “Convenção para a

repressão de atos ilícitos contra a segurança da navegação marítima" e de um protocolo para a "Repressão de atos ilícitos contra a segurança de plataformas fixas localizadas na Plataforma Continental". [69]

Pode-se dizer que assim iniciou-se o combate ao terrorismo no mundo, não de forma sistemática, mas através de ações isoladas que permitiriam, no futuro, uma maior efetividade no combate ao terrorismo.

Pode-se dizer que assim iniciou-se o combate ao terrorismo no mundo, não de forma sistemática, mas através de ações isoladas que permitiriam, no futuro, uma maior efetividade no combate ao terrorismo.

Com o crescente número de ataques terroristas, sobretudo após os atentados contra o Pentágono e às torres gêmeas em 11/09/2001, as organizações do Sistema das Nações Unidas mobilizaram-se em suas respectivas esferas para intensificar a luta contra o terrorismo. Em 28 de setembro do mesmo ano, o Conselho de Segurança adotou a Resolução 1373, nos termos de aplicação da Carta da ONU, para impedir o financiamento do terrorismo, criminalizar a coleta de fundos para este fim e congelar imediatamente os bens financeiros dos terroristas. Ele também estabeleceu um Comitê Antiterrorismo para supervisionar a implementação da resolução.

Que implicações os ataques ao Pentágono e ao World Trade Center (WTC) apresentam para os Estados Unidos e para as relações internacionais? Quais seriam suas consequências para a ordem mundial deste início do século XXI? Cabe, com efeito a pergunta sobre se os eventos de 11 de setembro teriam, de fato, transformado a ordem global a ponto de constituir um divisor de águas na política mundial.

Os eventos de 11 de setembro de 2001 foram e têm sido apresentados como um momento de ruptura no sistema das relações internacionais, ou pelo menos como um

---

[69]Neto, José Cretella, Terrorismo Internacional-Inimigo sem rosto – Combatente sem pátria. 1ª Edição, Brasil, Ed. Millennium, 2008, ps 561 ss..

elemento novo na agenda da política mundial, ponto definidor de uma nova relação dos Estados Unidos com a ordem global, em grande medida dominada por esse mesmo país. Mesmos os países situados em área relativamente imune à ação do terrorismo de base fundamentalista, também passaram a sofrer as consequências da situação criada a partir da reação dos EUA a esses ataques.

Uma análise preliminar e introdutória aos problemas do 11 de setembro e de seu status na política americana e mundial confirmaria que, como quaisquer outros fenômenos históricos, estes possuem, ao mesmo tempo, elementos de ruptura e de continuidade. O mundo pós 11 de setembro não mudou, mas a agenda da política mundial modificou-se, não tanto pela ação em si dos terroristas como pela demonstração da vontade de poder da maior potência de nossa época.

Os trágicos acontecimentos na América também revelaram o perigo potencial das armas de destruição em massa nas mãos de agentes não-estatais. O ataque poderia ter sido ainda mais devastador se os terroristas tivessem acesso a armas químicas, biológicas e nucleares. Refletindo estas preocupações, a Assembleia Geral adotou, em 2002, a Resolução 57/83, primeiro texto contendo medidas para impedir terroristas de conseguirem tais armas e seus meios de lançamento.

Em 2004, o Conselho de Segurança tomou sua primeira decisão formal sobre o perigo da proliferação de armas de destruição em massa, especialmente para os atores não-estatais. Agindo de acordo com as disposições da Carta, o Conselho adotou por unanimidade a Resolução 1540, obrigando os Estados a interromperem qualquer apoio a agente não-estatais para o desenvolvimento, aquisição, produção, posse, transporte, transferência ou uso de armas nucleares, biológicas e químicas e seus meios de entrega. Posteriormente, a Assembleia adotou a Convenção Internacional para a Supressão de Atos de Terrorismo Nuclear, aberta para assinatura em 2005.

O Escritório das Nações Unidas contra Drogas e Crime (UNODC), localizado em Viena (Áustria), conduz o esforço internacional para combater o tráfico de drogas, o crime

organizado e o terrorismo internacional. Ele analisa novas tendências da criminalidade e da justiça, desenvolve bancos de dados, divulga pesquisas globais, reúne e divulga informações, faz avaliações sobre as necessidades específicas de cada país e medidas de alerta sobre, por exemplo, o aumento do terrorismo.

Em 2002, o UNODC lançou seu Projeto Global contra o Terrorismo com a provisão de assistência técnica e jurídica aos países para tornarem-se parte e implementarem uma série de instrumentos contra o terrorismo. Em janeiro de 2003, o UNODC expandiu suas atividades de cooperação técnica para fortalecer o regime legal contra o terrorismo, prestando assistência técnica e jurídica para os países em tornar-se parte e implementarem os instrumentos universais antiterrorismo.

Na esfera jurídica, a ONU e seus órgãos – como a Organização da Aviação Civil Internacional (ICAO), a Organização Marítima Internacional (IMO) e a Agência Internacional de Energia Atômica (AIEA) – desenvolveram uma rede de acordos internacionais que constituem os instrumentos básicos legais contra o terrorismo.

Estes instrumentos incluem convenções sobre crimes cometidos a bordo de aeronaves; apoderamento ilícito de aeronaves; atos contra a segurança de civis; crimes contra pessoas protegidas internacionalmente, incluindo diplomatas; proteção física dos materiais nucleares; e a marcação de explosivos plásticos para fins de detecção. Além disso, eles incluem protocolos sobre atos de violência em aeroportos da aviação civil internacional, e sobre os atos contra a segurança de plataformas fixas localizadas no continente.

A Assembleia Geral também concluiu as cinco convenções seguintes: Convenção Internacional contra a Tomada de Reféns; Convenção sobre a Segurança das Nações Unidas e Pessoal Associado; Convenção Internacional para a Supressão de Atentados Terroristas; Convenção Internacional para a Supressão do Financiamento do Terrorismo; e a Convenção Internacional para a Supressão de Atos de Terrorismo Nuclear.

Infelizmente, grandes ataques terroristas continuaram após o 11 de setembro – incluindo ataques à sede da ONU em Bagdá (agosto de 2003); em quatro trens em Madrid (março de 2004); num escritório e em apartamentos em Al-Khobar, na Arábia Saudita (maio 2004); no metrô de Londres (julho de 2005); numa zona litorânea e num centro comercial em Bali (outubro de 2005); em vários locais de Mumbai (novembro 2008); nos hotéis Marriott e Ritz-Carlton em Jacarta (julho 2009), no metrô de Moscou (março 2010), para citar apenas alguns, e finalmente os atentados em Paris no final de 2015.

A posição adotada pelos EUA após o atentado sofrido, no que diz respeito ao terrorismo gerou consequências fundamentais na Europa. As medidas tomadas por George Bush refletiram na adoção de legislações específicas acerca do tema por países europeus, bem como enrijecimento das normas preexistentes, v. G., a Decisão-marco 2002/475/JAI editada pelo Conselho da União Europeia sobre a harmonização da legislação penal em matéria de terrorismo e mandado de prisão, sem prejuízo de outros projetos e ações no mesmo sentido.

Como parte do esforço internacional para conter esta onda mortal, a Assembleia Geral adotou por unanimidade e lançou, em 2006, a Estratégia Antiterrorista Global da ONU. Baseada na convicção fundamental de que o terrorismo, em todas as suas formas, é inaceitável e não pode nunca ser justificado, a Estratégia define uma série de medidas específicas para combater o terrorismo em todas suas vertentes, em nível nacional, regional e internacional. [70]

A 4 e 5 de setembro de 2008, a Assembleia Geral organizou a sua primeira reunião dedicada à análise da implementação da Estratégia Antiterrorista Mundial e adotou uma resolução em que reafirma o seu compromisso a favor dessa estratégia e da sua aplicação. Um dos contributos para esse processo foi o relatório elaborado pelo Secretário-Geral em 2008, sobre a ação do sistema das Nações Unidas. [71]

---

[70] https://nacoesunidas.org/acao/terrorismo/
[71] idem

Em 08 de setembro de 2010, a Assembleia Geral realizou a segunda revisão das Estratégias Antiterroristas das Nações Unidas. Numa resolução adotada por consenso, os Estados-Membros reiteraram a condenação veemente e inequívoca do terrorismo em todas suas formas e manifestações: “por quem quer que seja, onde e para que finalidades.

Os Estados-Membros também reafirmaram o apoio à Estratégia de quatro pilares: enfrentar as condições propícias à propagação do terrorismo, prevenção e combate ao terrorismo; construir a capacidade dos Estados para prevenir e combater o terrorismo e reforçar o papel do sistema das Nações Unidas nesse sentido; e garantir o respeito pelos direitos humanos para todos e do Estado de direito como a base fundamental para a luta contra o terrorismo.

O grande problema é que há um enorme conflito entre os diversos organismos internos da Organização das Nações Unidas, sobretudo entre a Assembleia Geral e o Conselho de Segurança, sem falar de outros, como a Corte Internacional de Justiça (com destacada atuação), o Conselho Econômico e Social, o Conselho de Tutela (quase sem funções, atualmente).

Este conjunto possui estrutura de difícil administração, sendo composto por sete órgãos principais aos quais estão subordinados cerca de 90 escritórios, agências, comitês, programas, fundos e outras entidades, com um número enorme de funcionários, o que afeta o processo de tomada de decisões.

Isso acaba influindo em desfavor da eficiência da ONU em relação ao terrorismo mundial, tornando-a contraproducente por duas razões principais:

a) faz com que governos hostis ao Ocidente substituam ações armadas estatais (guerras) que não poderiam vencer, por ataques terroristas através de auxílio financeiro indireto;

b) Impede e dificulta que os EUA e seus aliados usem seu poderio militar para elevar o “custo” desse apoio governamental de Estados inimigos a terroristas. Para assim diminuir a frequência dos ataques terroristas.

Faz-se necessário um esforço coletivo no sentido de unificar as posições dos diversos organismos, dotando apenas um de poderes para o efetivo combate ao terrorismo, sem o prejuízo do auxílio e assessoramento das demais entidades.

O combate ao terrorismo é conduzido em duas grandes vertentes: o antiterrorismo e o contraterrorismo. O antiterrorismo compreende a condução das medidas de caráter eminentemente defensivo e preventivo que objetivam a redução das vulnerabilidades aos atentados terroristas.

Já o contraterrorismo compreende a condução das medidas de caráter eminentemente ofensivo e repressivo, tendo como alvo as diversas organizações terroristas em presença, a fim de prevenir, dissuadir, ou retaliar atos terroristas.

É condição para assegurar-se a segurança no mundo que os Estado encontrem um mecanismo de natureza legal que os autorize o pleno uso de medidas anti e contra terroristas.

Assim, surge, o direito penal do inimigo desenvolvido pelo professor alemão Günter Jakobs, na secunda metade da década de 1990.

Jakobs, por meio dessa denominação, distingui um Direito Penal do Cidadão e um Direito Penal do Inimigo. O primeiro, em uma visão garantista, com observância de todos os princípios fundamentais que lhe são inerentes; o segundo, denominado Direito Penal do Inimigo, seria um Direito Penal despreocupado com seus princípios fundamentais, pois que não estaríamos diante de cidadãos, mas sim de inimigos do Estado.

O raciocínio seria o de verdadeiro estado de guerra, razão pela qual, de acordo com Jakobs, na guerra, as regras do jogo devem ser diferentes. O Direito Penal do Inimigo, conforme salienta, já existe em nossas legislações, gostemos ou não disso, a exemplo do que ocorre no Brasil com a lei que dispõe sobre a utilização de meios operacionais para a prevenção de ações praticadas por organizações criminosas (Lei no 9.034, de 3 de maio de 1995).

Segundo o referido autor, o Direito penal conhece dois polos ou tendências de suas regulações. Por um lado, o trato com o cidadão, em que se espera até que este exteriorize seu fato para reagir, com o fim de confirmar a estrutura normativa da sociedade, e por outro, o trato com o inimigo, que é interceptado prontamente em seu estágio prévio e que se combate por sua perigosidade.

Há pessoas, segundo Jakobs, que decidiram se afastar, de modo duradouro, do Direito, a exemplo daqueles que pertencem a organizações criminosas e grupos terroristas. Para esses, “a punibilidade se adianta um grande trecho, até o âmbito da preparação, e a pena se dirige a assegurar fatos futuros, não a sanção de fatos cometidos.

Existem pessoas que, por sua insistência em delinquir, voltam ao seu estado natural antes do estado de direito. Assim, um indivíduo que não admite ser obrigado a entrar em um estado de cidadania não pode participar dos benefícios do conceito de pessoa. E é que o estado natural é um estado de ausência de norma, quer dizer, a liberdade excessiva tanto como de luta excessiva. Quem ganha a guerra determina o que é norma, e quem perde há de submeter-se a essa determinação.

O Estado, conclui, “pode proceder de dois modos com os delinquentes: pode vê-los como pessoas que delinquem, pessoas que cometeram um erro, ou indivíduos aos que há de impedir mediante coação que destruam o ordenamento jurídico.

Manuel Cancio Meliá, analisando a proposta de Jakobs, esclarece:

Segundo Jakobs, o Direito penal do inimigo se caracteriza por três elementos: em primeiro lugar, se constata um amplo adiantamento da punibilidade, quer dizer, que neste âmbito, a perspectiva do ordenamento jurídico-penal é prospectiva (ponto de referência: o fato futuro), em lugar de – como é habitual – retrospectiva (ponto de referência: o fato cometido). Em segundo lugar, as penas previstas são desproporcionadamente altas: especialmente, a antecipação da barreira de punição não é tida em conta para reduzir em correspondência a pena ameaçada. Em terceiro lugar, determinadas garantias processuais são relativizadas ou, inclusive, suprimidas.[72]

É, sobretudo nessa assertiva, de relativização de garantias processuais que entendemos que se busca a relativização do direito ao silêncio.

Pressuposto do Estado de Direito Democrático é o reconhecimento do cidadão como como sujeito livre, capaz de decidir e de responder pelas suas decisões. Se uma pessoa é totalmente privada da sua capacidade de decisão e de autodeterminação, se a sua vontade é totalmente subjugada a uma vontade alheia, como sucede na tortura, ela não só não pode responder pelo que faz, como fica impossibilitado de escolher o seu destino individual e o seu destino coletivo. Faltando este pressuposto, em consequência da despersonalização do torturado, desaba, qual castelo de cartas, toda a base de legitimidade do Estado de Direito concebido democraticamente. Este pode restringir temporariamente a liberdade ambulatória de um cidadão que delinquiu, mas não pode privá-lo de toda a liberdade; pode obrigar o cidadão que delinquiu a trabalhar por um tempo (v.g. pena de trabalho a favor da comunidade) mas não pode reduzi-lo à escravidão; **pode deter e interrogar o cidadão suspeito da prática de crime, mas não pode forçá-lo a falar e, desse modo, a cooperar na sua autoincriminação e condenação** (grifo nosso). Se o fizer, seja em nome da segurança coletiva, da paz internacional, do combate ao inimigo ou de outra qualquer finalidade louvável, o Estado perde a sua natureza de «Direito» (deixa de haver sujeito livre, titular de direitos e destinatário de deveres, capaz de responder pelo exercício de uns e o cumprimento de

---

[72] Greco, Rogério. Direito penal do inimigo – Jus Brasil - https://rogeriogreco.jusbrasil.com.br/artigos/121819866/direito-penal-do-inimigo

outros) e «Democrático» (deixa de existir cidadão livre e capaz de participar na escolha do destino coletivo). Por isso, Estado de Direito Democrático (art. 2º da CRP) e dignidade da pessoa (art. 1º da CRP) são dois princípios co-originários, que se implicam reciprocamente.[73] Por isso também, a prática da tortura não colhe fundamento no quadro, já de si elástico, da proporcionalidade constitucionalmente conformada (art. 18 nº 2 da CRP) mas apenas fora dele, numa lógica de combate ao inimigo, de segurança efetiva a qualquer preço. O Estado de Direito Democrático não suporta dentro das suas fronteiras uma tal lógica de excepção e de guerra, associada a procedimentos e métodos próprios de organizações terroristas e de Estados totalitários.[74]

É preocupante que tal direito seja ameaçado em razão da conjuntura. Necessárias medidas devem ser tomadas, em nível mundial, posto que o problema é global, a fim de se buscar mecanismos que protejam o direito a não autoincriminação.

Não se trata apenas do terrorismo que aflige nossos legisladores e doutrinadores, do mesmo modo, as organizações criminosas, em sentido amplo, aí envolvendo, o tráfico de entorpecentes, o tráfico de armas, a prostituição internacional (envolvendo o tráfico humano) tem levado a doutrina penal a ampliar e criar conceitos penais e processuais penais visando soluções para o combate à criminalidade, quase sempre visando a supressão de direitos e garantias fundamentais como o direito ao silêncio.
O chamado Direito Penal do Inimigo encontra-se, hoje, naquilo que se reconhece como a *terceira velocidade do Direito Penal*. De acordo com o que se denomina *processo de expansão do Direito Penal,* podemos, seguindo as lições de Jésus-Maria Silva Sánchez, visualizar três velocidades, três enfoques diferentes que podem ser concebidos ao Direito Penal.

---

73 Essa co-originariedade está bem patente na conjugação necessária dos arts. 1º e 2º da CRP – v. GOMES CANOTILHO/VITAL MOREIRA, *Constituição Portuguesa Anotada*, art. 2º, I, (p. 203), afirmando que o art. 2º duplica o conteúdo do art. 1º, sob a perspectiva do Estado.

74 Dias, Augusto Silva. *Torturando o inimigo ou libertando da garrafa o gênio do mal? Sobre a tortura em tempos de terror.* Revista do Ministério Público do RS, Porto Alegre, n. 71, jan. 2012 – abr. 2012

A primeira velocidade seria aquela tradicional do Direito Penal, que tem por fim último a aplicação de uma pena privativa de liberdade. Nessa hipótese, como está em jogo a liberdade do cidadão, devem ser observadas todas as regras garantistas, sejam elas penais ou processuais penais.

Numa segunda velocidade, temos o Direito Penal à aplicação de penas não privativas de liberdade, a exemplo do que ocorre no Brasil com os Juizados Especiais Criminais, cuja finalidade, de acordo com o art. 62 da Lei no 9.099/95, é, precipuamente, a aplicação de penas que não importem na privação da liberdade do cidadão, devendo, pois, ser priorizadas as penas restritivas de direitos e a pena de multa. Nessa segunda velocidade do Direito Penal poderiam ser afastadas algumas garantias, com o escopo de agilizar a aplicação da lei penal.

Percebemos isso com clareza quando analisamos a mencionada Lei dos Juizados Especiais Criminais, que permite a utilização de institutos jurídicos que importem na aplicação de pena não privativa de liberdade, sem que, para tanto, tenha havido a necessária instrução processual, com o contraditório e a ampla defesa, como acontece quando o suposto autor do fato aceita a proposta de transação penal, suspensão condicional do processo, etc.

Assim, resumindo o raciocínio com Jésus-Maria Silva Sánchez, teríamos:
uma primeira velocidade, representada pelo Direito Penal ‘do cárcere’, em que haveriam de ser mantidos rigidamente os princípios político-criminais clássicos, as regras de imputação e os princípios processuais; e uma segunda velocidade, para os casos em que, por não se tratar de prisão, senão de penas de privação de direitos ou pecuniárias, aqueles princípios e regras poderiam experimentar uma flexibilização proporcionada a menor intensidade da sanção.

Embora ainda com certa resistência, tem-se procurado entender o Direito Penal do Inimigo como uma *terceira velocidade*. Seria, portanto, uma velocidade híbrida, ou seja,

com a finalidade de aplicar penas privativas de liberdade (primeira velocidade), com uma minimização das garantias necessárias a esse fim (segunda velocidade).
Na verdade, a primeira indagação que devemos fazer é a seguinte: Quem poderá ser considerado inimigo, para que vejam diminuídas ou mesmo suprimidas suas garantias penais e processual-penais?

Em muitas passagens de sua obra, Jakobs aponta como exemplo as atividades terroristas.[75]

10 - Conclusão

A exigência da necessária previsão normativa, como um dos pressupostos de toda medida limitadora de direitos fundamentais, estende-se ao estabelecimento do grau de rompimento de cada um dos pressupostos para entender como vulnerado o direito fundamental de que se trate, além do julgamento ponderativo correspondente entre os objetivos em tensão, a investigação do delito e a persecução dos especialmente graves, assim como a obrigação estatal de tutelar os direitos fundamentais.[76]

O que se deve discutir não é a possibilidade de o Estado restringir direitos fundamentais, e sim, em que extensão essa restrição pode ocorrer sem que se torne uma medida inconstitucional. Daí se conclui que o grande paradoxo do sistema penal é a convivência entre suas duas finalidades primordiais: a eficácia na realização da justiça e a proteção dos direitos fundamentais do cidadão.

Diante da impossibilidade de integral harmonia entre elas logrou-se atingir na maioria dos Estados Democráticos de Direito aquilo que Jorge de Figueiredo Dias chama de

---

[75] Greco, Rogério. Direito penal do inimigo – Jus Brasil - https://rogeriogreco.jusbrasil.com.br/artigos/121819866/direito-penal-do-inimigo

[76] Deu, Teresa Armenta*. A prova ilícita- um estudo comparado*.1.ed, São Paulo: Marcial Pons, 2014. [40] DIAS, Jorge de Figueiredo Dias, *apud* Greghi, Fabiana. NETO, Eduardo Diniz.*Relativização de direitos fundamentais: uma abordagem a lume da necessidade da adoção de um tratamento constitucional penal diferenciado face à expansão desenfreada da criminalidade organizada*. REVISTA DE DIREITO PÚBLICO, LONDRINA, V. 3, N. 2, P. 210-228, MAI/AGO. 2008.

“concordância prática” dessas finalidades em conflito, “de modo que de cada uma se salve, em cada situação o máximo conteúdo possível, otimizando os ganhos e minimizando as perdas axiológicas e funcionais” Ou seja, faz-se necessária a urgente normatização desse tipo de situação, cada dia mais usual, sob pena de o direito sucumbir ao arbítrio.

As afirmativas supra referidas corroboram a presente conclusão.

Como a tecnologia se torna cada vez mais associada a uma pessoa, tanto no sentido físico, quanto no que diz respeito a informações de natureza pessoal, nossos legisladores, doutrinadores e tribunais continuarão a enfrentar dilemas semelhantes.

Privacidade e informação não são mais conceitos estritamente, físicos, tangíveis. Quanto mais a tecnologia avança, mais o sistema jurídico terá de resolver questões de ponta na era digital. No entanto, muitas das nossas leis têm sido ultrapassadas e não têm disposições especiais para examinar com acurácia assuntos relativos a tecnologia digital e informações pessoais.

O desenvolvimento tecnológico conquistado pelas organizações visa a impedir a colheita de provas, uma vez que o Estado, desmuniciado ou carente de toda essa tecnologia, fica longe de ter êxito na persecução penal.

É neste sentido, portanto, que se faz necessária a restrição de certos direitos fundamentais dos acusados que se dá, por exemplo, por meio da quebra do sigilo bancário e fiscal, interceptação das comunicações ambientais e telefônicas, na tentativa de se conquistar maior eficiência penal ante a inadequação do sistema penal clássico em sede de delinquência organizada.

Com efeito, como as garantias e direitos fundamentais do cidadão, a ordem e a segurança pública também estão insculpidas no texto constitucional (artigos 5º, 6º e 14 da Constituição Federal) e não podem ser sacrificadas em virtude de uma concepção

simplesmente individualista. Além do que, conforme já mencionado, nenhum direito pode ser entendido como absoluto ou ilimitado. Os direitos fundamentais gozam de certa relatividade em razão da necessidade de se resguardar outros direitos fundamentais.[77]

Wagner Marteleto Filho nas considerações finais de sua obra "O direito à não autoincriminação no processo penal contemporâneo encerra seu magistério com palavras que inspiram o enceramento da presente dissertação: "No Processo penal democrático, a verdade não pode ser perseguida a qualquer preço, consistindo, os direitos fundamentais do acusado, limites éticos e normativos para a produção da prova.

Da presunção de inocência deriva que a carga probatória há de ser suportada pela acusação, não sendo dever do arguido cooperar com o Estado, auto incriminando-se. O princípio *nemo tenetur se degere* joga, aqui um papel decisivo, extremando os modelos processuais acusatório e inquisitivo, e estabelecendo qualquer contributo do arguido que resulte em desfavor de sua posição processual...

A necessidade imperiosa de se varrer a tortura do palco do processo, no ideário iluminista, fez com que o acusado fosse brindado e blindado com o direito ao silêncio, no sentido de que suas manifestações de cunho testemunhal não mais pudessem ser extorquidas pelo inquisidor, obsessivamente comprometido com a confissão.[78]

Na Virgínia, o que está claro agora é que você deve proteger o seu smartphone usando uma senha, não a sua impressão digital.[79]

---

[77] Greghi, Fabiana.Neto, Eduardo Dniz. Relativização de direitos fundamentais: uma abordagem a lume da necessidade da adoção de um tratamento constitucional penal diferenciado face à expansão desenfreada da criminalidade organizada. Revista do Direito Público. Universidade Estadual de Londrina - http://www.uel.br/revistas/uel/index.php/direitopub/article/view/10948/9622

[78] Filho, Wagner Marteleto – O Direito à não autoincriminação no processo penal contemporâneo. P.208, 1ªed. Editora Del Rey, 2012, p.234/235.

[79] BODI, Anna E.*Smartphones, fingerprints and the fifith amendment*. American Criminal Law Review,

A decisão do Juiz Frucci preserva a esperança de que o princípio do *nemo tenetur se detegere* continue nos abrigando como abrigou a todos desde seu desenvolvimento através dos tempos.

Bibliografia

ALBUQUERQUE, Marcelo Schirmer*. A garantia de não auto-incriminação extensão e limites*. Belo Horizonte: Del Rey, 2008.

BELEZA, Teresa Pizarro. PINTO, Frederico de Lacerda da. Coordenação*. Prova criminal e direito de defesa – Estudos sobre teoria dea proa e garantias de defesa em processo penal.*Ed. Almedina. 2ª Reimpressão. 2013.

BODI, Anna E*. Smartphones, fingerprints and the fifith amendment*. American Criminal Law Review, 2016

BOTTINO, Thiago*. A doutrina brasileira do direito ao silêncio - o STF e a conformação do sistema processual penal constitucional*. São Paulo: Campus Jurídico, 2008.

BRESSAN, Kelvin J. É necessária autorização judicial para exame dos dados armazenados em um smartphone?: emporiododireito.com.br/leitura/e-necessaria-autorizacao-judicial-para-exame-dos-dados-armazenados-em-um-smartphone-uma-breve-analise-do-rhc-n-51-531-ro-do-superior-tribunal-de-justica

CANOTILHO, J,J, Comentários à Constituição do Brasil / J. J. Gomes Canotilho...[et al.] ; outros autores e coordenadores Ingo Wolfgang Sarlet, Lenio Luiz Streck, Gilmar Ferreira Mendes. – 2. ed. – São Paulo : Saraiva Educação, 2018.

CARNEIRO, Leandro Dias, Infrações penais e a informática: a tecnologia como meio para o cometimento de crimes, Revista Âmbito Jurídico - No 168 - Ano XX - ABRIL/2018 - ISSN - 1518-0360

CONSTABLE, Mariane. *Just silences: the limits and possibilities of modern law*. Princeton University Press. 2005.

TERZIAN, Dan*. Forced decryption as equilibrium-why it's constitutional and how riley matters [dagger]*. Northwestern University Law Review, Vol. 109, No. 4, 2015.

DERSHOWITZ, Alan M. *Is there a right to remain silence? Coercive interrogation and the fifth amemdment after 09/11*. New York: Oxford University Press, 2008.

DEU, Teresa Armenta. *A prova ilícita- um estudo comparado*.1.ed, São Paulo: Marcial Pons, 2014.

DEZEM, Guilherme Madeira. *A proteção da intimidade e os tribunais internacionais*. In: RASCOVSKI, Luis (coord.). Temas relevantes de Direito Penal e Processual Penal. São Paulo: Saraiva, 2012.

DIAS, Augusto Silva. Torturando o inimigo ou libertando da garrafa o gênio do mal? Sobre a tortura em tempos de terror. Revista do Ministério Público do RS, Porto Alegre, n. 71, jan. 2012 – abr. 2012

DIAS, Augusto Silva/Ramos Vânia Costa, O Direito à Não Auto-Inculpação (Nemo Tenetur Se Ipsum Accusare) no Processo Penal e Contra-Ordenacional Português edição: Coimbra Editora, setembro de 2009.

DIAS, Jorge de Figueiredo. Andrade, Manuel do Costa. Supervisão, Direito ao Silêncio e legalidade da prova. Ed. Almedina. 1ª ed. 2009. P. 38

DIAS, Jorge de Figueiredo Dias, apud Greghi, Fabiana. NETO, Eduardo Diniz. *Relativização de direitos fundamentais: uma abordagem a lume da necessidade da adoção de um tratamento constitucional penal diferenciado face à expansão desenfreada da criminalidade organizada*. Revista de Direito Público, Londrina, V. 3, N. 2, P. 210228, MAI/AGO. 2008.

FERNANDES, Antônio Scarance.ALMEIDA, José Raul Gavião de. MORAES, Maurício Zanóide de. Coordenação. *Provas no Processo Penal – Estudo comparado*. Ed. Saraiva 2011.

FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Cadernos de Direito Tributário e Finanças Públicas, nº 1, São Paulo: RT, 1992. p. 141-154

GOMES, Luiz Flávio*. Princípio da não auto-incriminação: significado, conteúdo, base jurídica e âmbito de incidência.* Disponível em http://www.lfg.com.br 26 janeiro. 2010.

GOMES, Luiz Flávio. *Princípio da não autoincriminação: significado, conteúdo, base jurídica e âmbito de incidência*. Disponível em http://www.lfg.com.br 07 janeiro. 2016.

GOMES, Luiz Flávio*. Crime organizado: que se entende por isso depois da Lei 9.034/95. (Apontamentos sobre a perda da eficácia de grande parte da Lei 9.034/95).* Disponível em:<http://www.jus.br/doutrina/texto.asp? id=2919>. Acesso em: 25 mar. 2007.

GREGUI, Fabiana.Neto, Eduardo Dniz. Relativização de direitos fundamentais: uma abordagem a lume da necessidade da adoção de um tratamento constitucional penal diferenciado face à expansão desenfreada da criminalidade organizada. Revista do Direito Público. Universidade Estadual de Londrina

GRISWOLD, Erwin N. *The 5th Amendment Today: Three Speeches*. Harvard University Press, 1955.

Harvard Journal of Law and Technology

http://www.brc.com.br/juiz-federal-diz-que-reus-nao-podem-ser-forcados-a-revelarsenhas/

https://nacoesunidas.org/acao/terrorismo/

INBAU, Fred E. *Should We Abolish the Constitutional Privilege against SelfIncrimination?* Journal of Criminal Law and Criminology, Vol. 89, No. 4, Summer 1999.

JESUS, Francisco Marcolino de. *Os meios de obtenção da prova em processo penal*, Ed. Almedina. 2015.

JORGE DE FIGUEIREDO DIAS/MANUEL DA COSTA ANDRADE, (Parecer) in Supervisão, direito ao silêncio e legalidade da prova (CMVM) Almedina, Coimbra, 2009, pp. 44/45.

LaFAVE, Wayne R. Israel, Jerold H.King, Nancy J. Kerr, Orin S. *Criminal Procedure.* Série HORNBOOK. Ed. 2015.

LIMA, Aldo Corrêade. PRINCÍPIO DA NÃO AUTO-INCRIMINAÇÃO (DIREITO AO SILÊNCIO, POR EXEMPLO). https://aldoadv.wordpress.com/2010/01/26/principio-danao-auto-incriminacao-significado-conteudo-base-juridica-e-ambito-de-incidencia/

MARQUES, José Frederico. Elementos de Direito Processual Penal. 2ª ed. Rio de Janeiro. Ed. Forense. 1961

MARTINS, Milene Viegas . A Admissibilidade de Valoração de Imagens captadas por particulares comp prova no processo penal penal, Ed. Associação Acadêmica da Faculdade de Direito de Lisboa. 1ª ed. 2014.

NETO, José Cretella, Terrorismo Internacional-Inimigo sem rosto – Combatente sem pátria. 1ª Edição, Brasil, Ed. Millennium, 2008, ps 561 ss..

NUCCI, Guilherme de Souza. Provas no Processo Penal.Ed. Forense. 4ª edição. 2015

OLIVEIRA, Ronielton Rezende. Criptograria simétrica e assimétrica: os principais algoritmos de cifragem, Publicado na Revista online com distribuição gratuita Segurança Digital em duas partes: 5ª Edição – páginas 11 à 15 (31 de março de 2012) e 6ª Edição – páginas 21 à 24 (31 de maio de 2012).

O'REILLY, Gregory W*. England Limits the Right to Silence and Moves towards an Inquisitorial System of Justice*. Journal of Criminal Law and Criminology. Vol. 85, No. 2. 1994

PACHECO, Denilson Feitoza, Princípio da proporcionalidade no direito processual penal, http://www.cartaforense.com.br/conteudo/artigos/principio-da-proporcionalidade-no-direito-processual-penal/4208.

PAULO, Leonardo Costa de*. Autoincriminação e ilicitude na obtenção da prova –A limitação do Poder*. Revista Eletrônica de direito processual. Vol.4., 2009. Disponível *em:<http://www.arcos.org.br/periodicos/revista-eletronica-de-direito-processual/volume-iv/auto-incriminacao-e-ilicitude-na-obtencao-da-prova-a-limitacao-do-poder>*

QUEIJO, Maria Elizabeth*. O direito de não produzir prova contra si mesmo – o princípio nemo tenetur se detegere e suas decorrências no processo penal*. 2ª ed. Editora Saraiva. 2012

ROBINSON, Jeffrey*. A globalização do crime.* Rio de Janeiro: Ediouro, 2001.

SOARES, Nicholas. *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*. American Criminal Law Review, vol. 49, nº4, 2012

Shekhtman, Lonnie - Telefones vulneráveis ao rastreamento de localização, mesmo quando o GPS está desativado

SOUZA, Sérgio Ricardo de. Manual da Prova Penal Constitucional, 3ª Edição. Editora Juruá, 2017.

Terzian, Dan. The Micro-Hornbook on the Fifth Amendment and Encryption. https://georgetownlawjournal.org/articles/151/micro-hornbook-fifth-amendment-encryption.

Citation: 104 Geo L.J. Online 168 (2016)

- www.princeton.edu/news/2017/11/29/phones-vulnerable-location-tracking-even-when-gps-services

WINKLER, Andrew T. *Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technological Era*. Rutgers Computer & Technology Law Journal, Vol. 39, No. 2, Fall 2013.

www.brc.com.br/juiz-federal-diz-que-reus-nao-podem-ser-forcados-a-revelar-senhas/

www.dizerodireito.com.br/2018/08/lei-137092018-lei-geral-de-protecao-de.html

ANEXO I

COMM0MWEALTH OF VIRGINIA

SECOND JUDICIAL CIRCUIT

October 28, 2014

CIRCUIT COURT .JUDG
OFFIGE CITY OF VIRGINIA
BEACB JUDICIAL CENTER,
BLDG. 10 2425**NIMMO PARKWAY** VJRGINJA
BEACH, VA 23456-9017
(757) 385-4501
www.v
ov.com/conrts
Dlrect**Dial** # **385-8680**

Eleanor Gaines, Esquire
Office of the Commonwealth's
Attorney 2425 Nimmo
Parkway
Building 10B,
Seconc:J Floor
Virgínia Beach, VA
23456

James O.
Broccoletti, Esquire
Zoby, Broccoletti &
Normile, P. C. 6633
Stoney Point South
Norfolk, VA 23502

Re: Commonwealth of Virglnia v. David Charles Baust Docket No.: CR14-1439

Dear Counsel:

This matter is before the court on the Commonwealth's Motion to Compel the Production of the Passcode or Fingerprint to Ençrypted Smartphone. The heanng took place Tuesday, October 28, 2014, at which the Defendant, the Commonwealth, and the witness for the Commonwealth were present. For the reasons set forth below, the Motion is d nied in *part* and granted in part.

David Charles Baust, Defendant, is charged by indictment with violat'ing Codé of Virginia § 18.2 51.6, Strangling Another Causing Wounding or lnjury. On February 19; 2014, Defendant allegedly assaulted the victim in his bedroom at his house. The victim stated that Defendant maintained a recording device that continuously recorded in the roam where the assault purportedly took place. On the moming of February 19, 2014, after being assaulted the victim states she went to grab the vídeo equipment from its usual place and Defendant assaulted her again to prevent her from taking the equipment. The victim stated that Defendant had previously transmitted vídeo footage to her through text messaging of the victim and himself engaging in sexual intercourse in his roam. The victim additionally admitted that the vídeo recorder transmits to Defendant's smart phone. Pursuant to a search warrant executed several days later, the police were able to recover the phone, several recording devices, assorted discs,

flash drives, and computer equipment belonging to Defendant. The victim and Defendant both affirmed to the officers at the scene that the recording device, connected to Defendant's cell phone "could have possibly" recorded the assault and the recording "may exist" on the phone. Additionally, the testimony before the court fróm the victim was that the device "could have recorded" the assault and therefore there "may be a recording." Entry to the phone has been prevented by encryption either by passcode or fingerprint.

The question before the court is whether the production of one's passcode or fingerprint is testimonial communication and therefore subject to the defendant's Fifth Amendment privilege against self-incrimination. The Commonwealth argues that the

passcode and' the fingerprint are not'tesfimoníâl becal..i'se the éxistence ofihe recording is a "foregone conclusion." Defense Counsel argues that both àre testimonial ih that either would provida access to all recordings ôr items on Defendant's phone.

Analysis

The Fifth Amendment to the Constitution of the United States provides that no person '"shall be compelled in any criminal case to be a witness against himself." U,S. Const. amend V. "[nhe Fourteenth Amendment secures ag inst state invasion the sarne privilege thát the Fifth Amendment guarantees against federal infringerrient - the right of a persori to remain silent unless he chooses to speak in the unfettered exercise of.his own will." *Schmerber v. Cal.,* 384 U.S. 757, 760 (1966) (citation amitted). "[í]he privilege protects an accused only from being compelled to testify against himself, or otheJWise provide the· State with évidence o·f a testimoníal or communicative nature." *U.S. v. Wade,* 388 U.S. 218, 221 (1967) (citation omitted). Thus the proper inquiry requires the court to resolve whether granting the motion to compel "would require (1) compulsipn of a (2) testimonial communication that is (3) incriminating." *U. S v. Authement,* 607 F.2d 1129, 1131 n.1 (5th Cir.1979).

It is a "settled. proposition that a person may be required to produce specific documents even thõUgh théy' conta,n incrimi rtating ass'ertions of faot or beliet beca the eation of those docum.ents was not 'compelled' within the meaning of the pnvilége [against self-incrimination]." *United States v. Hubbe/1,* 5.30 U.S. 27, 35-36 (2000); *accord Fisher v. United States,* 425 U.S. 391, 401 (1976) ("[T]he *Fífth Amendment* protects against icompelled self-incrimination, not the disclosure of private information'j. Thus the contents of the phone, obtaíned pursuant to a validly executed warrant are only subject to objections raised under the *Fourth Amendment,* not the *Fiftl:J Amendment.* Additi.onally, there is no question that a motion to compel is compulsive

and the production of the passcode or fingerprint wo.uld be incriminating. [1] The analysis tums on whether a passcode ora fingerprint is "testimonial communicatiôn."

---

[1] Incriminating has been defined as "any disclosures that the witness reasonably believes could be used in a criminal prosecution ar could lead to other evidence that might be so used." *Kastigar v. United States,* 406 U.S. **441,** 445 (1972).

Passcode or Fingerprint

"An act is testimonial when the accused is forced to reveal his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the govemment.;_ *U.S. v. Kirschner,* 823 F. Supp. 2d 665, 668 (2010) (citing *United States v. Doe,* 487 U.S. 201, 212 (1987)). "[I]here is a significant difference between the use of compulsion to extort communications from a defendant and cornpelling a person to engage in conduct that may be incriminating." *Hubbe/1,* 530 U.S.at 35. "[T]he privilege offers no protection against compulsion to submlt to fingerprinting, photography, Qr m easuremerits, to write or spéak for identfficátíon; to appear in court, to stand, to assl)me a stance, to walk, or to make a particular gesture." *Wade,* 388 U.S. éit 223 .

"tE)ven though the act may provide incriminating evidence, a criminal suspect may be com lied to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice. The act of exhlbitin·g such physical characteristics is not the sarne as a swom communication by a witness that relates either express or implied assertions of fact or belief." *Hubbe/1,* 530 U.S. at 35.

A witness's "act of production itself could quàlify as testimonial if conceding the existence , possessioh and control, and .authentici·ty of the documents tend[s] to incriminate [him or her]." *United States v. Doe (ln re Grand Jury Subpoena Duces Tecvm),* 6-70 F.3d 1335, 1343 (11th Cir. 2012) (citing holdi'ng of *Fisher v. United States,* 425 U.S. 391, 410 (1976)). Neverthéless, "[w]hen the 'existence and location' of the documents under subpoena are a 'foregone conclusion' and the witness 'adds little or nothing to the sum total of the Govemment's information by conceding that he in fact has fhe [documents],' then no Fifth Amendrnent right is touched because the 'question is hot of testimony but of surrender.'" *Doe v. United States (ln re Grand Jury Subpoena),* 383· F".3d 905, 91ó (9th Cir. 2004) (citing *!=isher,* 425 U.S. af 411) . "[f]he Govérnmerit is in· no way relying on the 'truthtelling ' of the [witness) to prove the existence of or his access to the documents." *Fisher,* 425 U.S. at 411. 'Whether the existence of do Li.rnents is a foregone conclu$ion is a que$tion ·o f fa et, sul;>j ct to revieW für clear error.D *United States v. Norwóod,* 420 F.3d 888, 895 (8th Cir.' 2005) (citihg *United States v. Doe,* 425 U.S. 605, 613-14 (1984).)

Therefore in *Hubbe/1,* the Court found the action of producing documents in response to a subpoena was testimonial in nature and therefore subject to the constitutional privilege against self-incrimination. *Hubbe/1,* 530 U.S. at 40. The Court was persuaded by the fact that in the act of production, the respondent had to take "the mental and physical

steps necessary to provide the prosecutor with an accurate inventory of the many sources of potentially incriminatiag evidence sought by the subpoena." ld. at 42. The Court reasoned that given this information, "[bJy 'producing documents in compliance with a subpoena, the witness wquld admit that the papers existed, were in his possession or control, and were authentic.' Moreover, ... when the [witness] responds to the subpoena, he may be compelled to take the witness stand

and answer . . . whether he has produced everything demanded by the subpoena." ld. at 36--37. The Court found notable that the text of the subpoena, often using the phrase "any and all documents related," made it obvious that the prosecutor needed respondent's assístance to identify potential sources of informaUon and to produce those sources of information. ld. at 41. Therefore, when the respondent produced these documents in response to the subpoena, it was the "functíonal equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition." ld, at 41-4 2. "The assembly of those documents was like tellíng an inquisitor the combination to a wall safe, not like being forced to surren er the ey to a strongbox." Further, the HubbeJI Court found t at the"foregone conclusfon" doctrine did no·t apply in thls case, where thé Govemment hâd not shown

that it had any prio·r knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent." ld. at 45.

Similarly, in the context of compelling the production of a passéode, the U.S. District Court for the Eastern District of Michigan held that compellíng the defendant to provide a password is a testimonial communication. *Uriited States v. Kirschner,* 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010). The court reasoned "forcing the Defendant to reveal the password . . . requires Oefendant to communic.ate 'knowledge,' unlike the

production of a handwriting sarnple o–r a voice exemplar." */d.* "lt is the 'extortion of

information *ftom* the accused,' the attempt to force him to 'disclose the contents of his owli mínd ' that- implicates lhe .*Self-lncrimination Cfause.*· " */d* . (quoting *United States v. Doe,* 487 U.S. ·at 211) (emphasis in origina.!). The court found *Hubbell's* distinction between telling an inquisitor the combination to a wall safe and surrendering a key to a strongbox instructive. */d.* Similar to having to divulge the combination to a safe, the court reasoned "the govemment is not seeking documents or objects - it is seeking testimony from the Defendant, requiring him to divulge through his mental processes his password." */d.; accord In re Grand Jury Súbpoena (Boucher),* No. 2:06-mj-91, 2007 U.S. Dist. LEXIS 87951 at *16, 2007 WL 4246473 (D. Vt. Nov. 29,. 2007) ("Since the government is trying to compel the pmduction -of the password. itself, the foregcme concJusion doctrine cannot ap ly. The p3SS\vord ·is n-ot a physicaJ thing,. Jf Ek>u er knows the password, it only exists in his mind.").[2]

ln this case, the Defendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the sarne . The footage itself would not be protected ·under the Fifth Arnendment because its creation was voluntary,

i.e. not compelled. As stated above, the *Fifth Amendment* only protects against "compelled" self-incrimination, therefore the contents of Defendant's

[2] However, on appeal, the District Court for the District of V rmonf found that requiring Defendant to produce an unencrypted version of the documents in his encrypted hard drive that he had already provided access to previously was not teslimonial because the existence of and location of the documents were a "foregone conclusion." *In re Grand Jury Sübpoena to Boucher,* 2009 U.S. Dist LEXIS 13006 at •a, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

phone, created voluntarily, are not protected against disclosure. However, compelling Defendant to provide access through his passcode is both compelled and testimonial and therefore protected. Contrary to the Commonwealth's assertion, the password is not a foregone conclusion because it is not known outside of Defendant's mind. Unlike a document or tangible thing, such as an unencrypted copy of the footage itsetf, if the password was a foregone conclusion, the Co.mmonwealth would not need to compel Defendant to produce it because they would already know it. As reasoned in *Kírschrier,* Defendant cannot be compelled to "divulge through his mental processes" the passcode for entry. The fingerprint, like a key, however; does not require the witness to divutge anything through his menta! proCêsses . On the contrary,.like physical characteristics that are non-testimonlal, thê fingerprint ôl U ete ndant if used to actess his pholie is likewisé hon testimonial and does not require Defendant to "communicate any knowledge" at alt Unlike the production of physical characteristic evidence, such as a fingerprint, the production of a pélssword forces the Defendant to "disclose the contents of his own mind.n For this reason the motion to compel the passcode should be **DENIED** but the motion tó compel the fingerprint should be **GRANTED.**

Unencrypted Footage

Neither has the Commonwealth asked to compel the unencrypted video recording. However, from the testimony of the witness at the tiearing, the exrstence and location of the recording is not a foregone conclusion and compelling Defendant to produce an unencrypted version would be self-incriminating. The most the Commonwealth knows is that the recording "cóu)d exist" because the device "may have recorded" the assault and transmitted it to the phóne. The altemative is also true, that the device "may not have" recorded the assault and the recording "may not exist." This being the only reason the Commonwealth suspects there may be à recording, the e:xistence and location of the retording is not a foregone conclusion. Defendant's production of the unencrypted recording.would be testimonial because Defendant would be admitting the recording exists, it was his possession and control, and that the recording is authentic. Therefore, the Commonwealth could not çompel Defendant to produce an unencrypted version of the recording.

Sincerely,

Steven e. Frucci Presiding Judge

Re: Commonweatih of Virginia v. David Charles Baust
Docket No.: CR14-1439
October 28, 2014

General Case Information Case Number CR1400143900 Parties Party Party Type commonwealth of virginia prosecutor baust, david charles defendant information defendant

Defendant DOB Sex City State
BAUST , DAVID CHARLES 10/9 M VIRGINIA BEACH VIRGINIA
Scheduling Information
Session Date
Scheduled
Party Scheduled Charge
Appearance Reason
Hearing
Result Comment
baust , david charles
unlawful woundingstrangle another causing wounding or injury
determination of counsel
felony 02/19/2014 NOT GUILTY 06/03/2015 (grifo nosso)

phone, created voluntarily, are not protected against disclosure. However, compe Defendant to provide access through his passcode is both compelled and testim and therefore protected. Contrary to the Commonwealth's assertion, the passwo not a foregone conclusion because it is not known outside of Defendant's mind. Unli document or tangible thing, such as an unencrypted copy of the footage itself, i password was a foregone conclusion, the Commonwealth would not need to co Defendant to produce it because they would already know it. As reasoned in *Kirsch* Defendant cannot be compelled to "divulge through his mental processes" the passc for entry. The fingerprint, like a key, however, does not require the witness to div anything through his mental processes. On the contrary, like physical characteris that are non-testimonial, the fingerprint of Defendant if used to access his phon likewise non-testimonial and does not require Defendant to "communicate knowledge" at all. Unlike the production of physical characteristic evidence, such fingerprint, the production of a password forces the Defendant to "disclose the cont of his own mind." For this reason the motion to compel the passcode should be **DEN** but the motion to compel the fingerprint should be **GRANTED**.

Unencrypted Footage

Neither has the Commonwealth asked to compel the unencrypted vi recording. However, from the testimony of the witness at the hearing, the existence location of the recording is not a foregone conclusion and compelling Defendan produce an unencrypted version would be self-incriminating. The most Commonwealth knows is that the recording "could exist" because the device "may h recorded" the assault and transmitted it to the phone. The alternative is also true, the device "may not have" recorded the assault and the recording "may not exist." being the only reason the Commonwealth suspects there may be a recording, existence and location of the recording is not a foregone conclusion. Defenda production of the unencrypted recording would be testimonial because Defendant wo be admitting the recording exists, it was in his possession and control, and that recording is authentic. Therefore, the Commonwealth could not compel Defendan produce an unencrypted version of the recording.

Sincerely,

Steven C. Frucci
Presiding Judge

SCF/alg/nc

Re: Commonweatih of Virginia v. David Charles Baust
Docket No.: CR14-1439
October 28, 2014

---

phone, created voluntarily, are not protected against disclosure. However, compe Defendant to provide access through his passcode is both compelled and testim and therefore protected. Contrary to the Commonwealth's assertion, the passwo not a foregone conclusion because it is not known outside of Defendant's mind. Unli document or tangible thing, such as an unencrypted copy of the footage itself, i password was a foregone conclusion, the Commonwealth would not need to co Defendant to produce it because they would already know it. As reasoned in *Kirsch* Defendant cannot be compelled to "divulge through his mental processes" the passc for entry. The fingerprint, like a key, however, does not require the witness to div anything through his mental processes. On the contrary, like physical characteris that are non-testimonial, the fingerprint of Defendant if used to access his phon likewise non-testimonial and does not require Defendant to "communicate knowledge" at all. Unlike the production of physical characteristic evidence, such fingerprint, the production of a password forces the Defendant to "disclose the cont of his own mind." For this reason the motion to compel the passcode should be **DEN** but the motion to compel the fingerprint should be **GRANTED**.

Unencrypted Footage

Neither has the Commonwealth asked to compel the unencrypted vi recording. However, from the testimony of the witness at the hearing, the existence location of the recording is not a foregone conclusion and compelling Defendan produce an unencrypted version would be self-incriminating. The most Commonwealth knows is that the recording "could exist" because the device "may h recorded" the assault and transmitted it to the phone. The alternative is also true, the device "may not have" recorded the assault and the recording "may not exist." being the only reason the Commonwealth suspects there may be a recording, existence and location of the recording is not a foregone conclusion. Defenda production of the unencrypted recording would be testimonial because Defendant wo be admitting the recording exists, it was in his possession and control, and that recording is authentic. Therefore, the Commonwealth could not compel Defendan produce an unencrypted version of the recording.

Sincerely,

Steven C. Frucci
Presiding Judge

SCF/alg/nc

Re: Commonweatih of Virginia v. David Charles Baust
Docket No.: CR14-1439
October 28, 2014